NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

IEEE 802.11 WIRELESS LOCAL AREA NETWORK SECURITY THROUGH LOCATION AUTHENTICATION

by

J. D. Morrison

September 2002

Thesis Advisor: J. D. Fulp
Second Reader: Dan Boger

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 2002	Master's Thesis

4. TITLE AND SUBTITLE IEEE 802.11 Wireless Local Area Network Security through Location Authentication

5. FUNDING NUMBERS

6. AUTHOR (S) J.D. Morrison

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Information Warfare Curriculum Office
Naval Postgraduate School
Monterey, CA

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the U.S. Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution authorized to DoD and DoD Contractors only; contains research applicable to military operations; 27 October 2002. Other requests for this document must be referred to Superintendent, Code 0052, Naval Postgraduate School, Monterey, CA 93943-5000 via the Defense Technical Information Center, 8725 John J. Kingman Rd., STE 0944, Ft. Belvoir, VA 22060-6218

12b. DISTRIBUTION CODE

13. ABSTRACT ***(maximum 200 words)***

The IEEE 802.11b wireless Local Area Network architecture was designed to make associations between host access points and client mobile users as simple and fluid as possible. This gives the system tremendous flexibility, but results in vulnerability to illicit network connections by unauthorized users. The ability of network intruders with high gain antennas to establish anonymous connections while maintaining a comfortable stand off distance constitutes a threat that must be countered before operating a wireless LAN can be deemed an activity with acceptable risks.

This thesis explores the possibility of using relative position with respect to the network access point as the determining factor in granting network access to potential mobile users. By analyzing the latency of layer two data acknowledgement control frames generated by the LAN adapter card one should be able to infer the relative distance between the 802.11b access point and any particular mobile user. From this knowledge, a policy that excludes potential users beyond a specified range can be implemented.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Wireless Local Area Networks, WLAN, IEEE 802.11, 802.11b, Information Assurance, Network Security, War Driving	110
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500 **Standard Form 298 (Rev. 2-89)**
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

IEEE 802.11 WIRELESS LOCAL AREA NETWORK SECURITY THROUGH LOCATION AUTHENTICATION

J. D. Morrison
Lieutenant Commander, United States Navy
B.S., Virginia Tech, 1985
M.A., University of San Diego, 1995

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2002

Author: J. D. Morrison

Approved by: J. D. Fulp
Thesis Advisor

Dan Boger
Second Reader

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The IEEE 802.11b wireless Local Area Network architecture was designed to make associations between host access points and client mobile users as simple and fluid as possible. This gives the system tremendous flexibility, but results in vulnerability to illicit network connections by unauthorized users. The ability of network intruders with high gain antennas to establish anonymous connections while maintaining a comfortable stand off distance constitutes a threat that must be countered before operating a wireless LAN can be deemed an activity with acceptable risks.

This thesis explores the possibility of using relative position with respect to the network access point as the determining factor in granting network access to potential mobile users. By analyzing the latency of the layer two data acknowledgement control frames generated by the WLAN adapter card one should be able to infer the distance between the 802.11b access point and any particular mobile user. From this knowledge, a policy that excludes potential users beyond a specified range can be implemented.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGEMENTS

The author gratefully recognizes the enthusiastic contributions of the following individuals whose efforts were instrumental to the completion of this thesis:

Jonathan Zweig of Nortel Networks for his adaption of the original LA model to a more effective layer two implementation within the IEEE 802.11 standard.

James Calusdian, NPS Optics and Servos lab engineer and Jeffrey Knight, NPS Circuits and Signals lab technician for their assistance with signal measurement equipment acquisition and training.

Robert Bluth, Richard Boyd and Robert Rogell of the NPS Center for Interdisciplinary Remotely Piloted Aircraft Studies (CIRPAS) for logistical coordination and use of their facilities in support of the thesis field-tests at the Marina Municipal Airport, Marina CA.

LCDR Daniel Widdis, NPS Operations Research department for his aid in the statistical analysis of the field-test data.

Dr. Daniel Boger of the NPS Information Sciences department for his insightful commentary and editing of the thesis drafts as second reader.

Professor J. D. Fulp of the NPS Computer Science department for his continual encouragement, guidance, and meticulous proofreading as primary thesis advisor.

Darwin Engwer of Nortel Networks for his erudite explanations to countless questions pertaining to the IEEE 802.11 standard, coordination of the necessary network hardware modifications, and facilitation of the initial lab testing.

Wendy and Miranda Morrison for their endless patience and support during the long hours spent apart over the past two years in pursuit of the education at NPS which made this culminating project possible.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

The fundamental design of the Institute of Electrical and Electronic Engineers (IEEE) 802.11b Wireless Local Area Network (WLAN) architecture is intended to make associations between host Access Point(s) (APs) and client mobile user(s) (MUs) as simple and fluid as possible. This gives the system tremendous flexibility, but results in vulnerability to illicit network connections by unauthorized users. The hazards of an open network are, of course, considerable. The ability to freely create associations with unprotected wireless networks enables unauthorized MUs to misappropriate network bandwidth, anonymously launch attacks on other networks through the wireless network's Internet connection, or launch insider attacks against the host network itself.

This is an inherent vulnerability in WLAN architecture that is being actively exploited by numerous ad hoc computer user groups around the country. The process of cataloging unprotected APs conducted by groups such as the Bay Area Wireless Users Group in San Francisco (and others) is known as "war driving". As can be clearly seen in Figure 1-1, the detailed information they provide presents a startlingly clear depiction of the possibilities for unauthorized access to numerous wireless networks throughout the city.

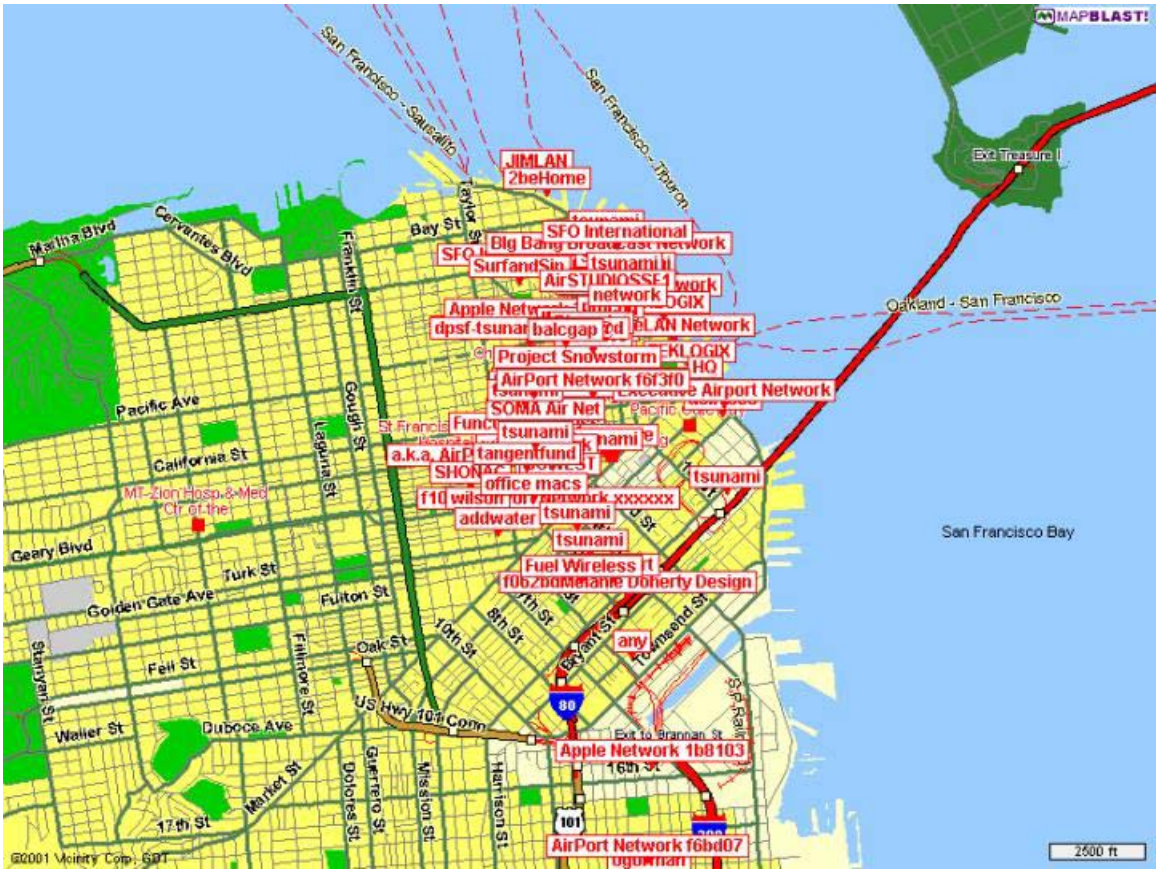

Figure 1.1 Unprotected Access Points Available for Exploitation in Downtown San Francisco (http://www.dis.org/wl/maps/)

In addition, some well meaning citizens of the net cooperate in permitting unfettered access to the web from their APs, allowing their location, channel number, and other helpful connection tips to be published as a “public service” to others. A search of the “Global Access Wireless Database” (http://www.shmoo.com/cgi-bin/gawd/gawd.cgi/) returns seventeen non-commercial entries for San Francisco alone. While many utilize this service for harmless web surfing, the anonymous access these APs provide can easily serve as a springboard for

network attacks by less scrupulous users for whom forensic efforts to discover their identity would be futile.

Exacerbating the problem of network intrusion is the ability of computer users with high gain antennas, connected to their WLAN cards, to establish connections at ranges well beyond those of legitimate users (as proven by LT Melvin Yokoyama's 2001 thesis: "Airborne Exploitations of an IEEE 802.11B Wireless Local Area Network"). Researchers on a more modest budget can easily find directions for building a directional antenna with 12dB gain from a simple potato crisp canister and about six dollars in readily obtained hardware on the Internet as illustrated in Figure 1-2.

Parts list:

All-thread, 5 5/8" long, 1/8" OD	$1.00
two nylon lock nuts	$0.10
five 1" washers, 1/8" ID	$0.10
6" aluminum tubing, 1/4" ID	$0.75
A connector to match your radio pigtail (we used a female N connector)	$3.00
1 1/2" piece of 12 gauge solid copper wire (ground wire from house electrical wiring)	$0.00
A tall Pringles can (any flavor)	$1.50
Scrap plastic disc, 3" across (like another Pringles can lid)	$0.00
Total:	**$6.45**

Figure 1.2 Homemade Directional Antenna (12 dB gain) Sufficient for Use at Ranges of up to Ten Miles (http://www.oreillynet.com/cs/weblog/view/wlg/448)

The ability of network intruders to establish anonymous connections while maintaining a comfortable stand off distance constitutes a threat that must be neutralized before operating a WLAN supporting the exchange of sensitive data can be deemed an activity with acceptable risks. Mr. Richard A. Clarke, National Coordinator for Security, Infrastructure Protection, and Counter-terrorism has gone on record recommending that "Until we have a better, proven track record with the wireless (networks), we all should shut them off until the technology gets better," (http://seattletimes.nwsource.com/html/businesstechnology/134504335_hack010.html). Given the runaway popularity of these devices however, that option does not seem at all realistic.

Although the 802.11b standard supports the use of 128 bit Wired Equivalent Privacy (WEP) link encryption, its effectiveness has been severely reduced by well publicized (and constantly improving) cracking methods. User authentication methods (such as RADIUS servers) constitute a good security approach, but may be rendered useless if the MU database is compromised. The defense in depth principle suggests that preventing unwelcome connections to the wireless network through the addition of a physical authentication factor (such as MU location) is a worthwhile pursuit.

B. PURPOSE

The intent of this thesis is to document a proof of concept study in which the distance between a host AP and a client MU may be inferred from the latency of a series of layer two data acknowledgement control frames sent from MU

to AP in response to a corresponding series of data frames initiated by the AP.

C. BENEFIT

If an AP can be made to recognize whether or not its MUs are operating from within a pre-defined service area, it should be possible to reduce the physical area over which a system administrator must be vigilant to a manageable size.

D. METHODOLOGY

Chapter II discusses selected aspects of the IEEE 802.11 standard, with an emphasis on Direct Sequence Spread Spectrum (DSSS) protocols and their application to wireless network user location authentication.

Chapter III offers a brief description of the existing security measures that have been incorporated into common practice to reduce the risk of network exploitation by unauthorized users.

Chapter IV introduces the concept of location authentication, addressing its potential (and attendant difficulties) as an information assurance tool in a single transmitter/receiver environment.

Chapter V describes the test design, implementation, and data evaluation carried out to determine the viability of location authentication on a wireless local area network.

Chapter VI summarizes the research findings, outlines requirements for a practical implementation of location authentication, and suggests methods for further development.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE IEEE 802.11 STANDARD

With respect to the International Standards Organization's (ISO) seven layer Open Systems Interconnection (OSI) model, the 802.11 standard directs only layer one (Physical) and layer two (Data Link or Medium Access Control (MAC)) specifications. The encapsulation of data within each successive layer enables all lower layers to function without regard for their higher layer payloads. This chapter is included in order to provide the reader with an understanding of the 802.11 layer one and two functions as they relate to location authentication.

A. PHYSICAL LAYER

Although IEEE 802.11 has become almost synonymous with DSSS wireless networks in the 2.4 GHz unlicensed Industrial Scientific and Medical (ISM) band, it is important to note that the standard also specifies two other physical layer protocols: 2.4 GHz Frequency Hopping Spread Spectrum (FHSS) and 900 nm infrared. Both have unique strengths and weaknesses compared to the DSSS. While the infrared version is limited to short range (10 to 20 meters), indoor installations; it works well in noisy RF environments and does not require line of sight. The frequency-hopping variant provides robust connectivity in virtually any RF environment with less power consumption than DSSS systems, but has an inherently slower throughput than DSSS. Recent extensions to the original DSSS standard (discussed below), coupled with its extended range capability and throughput advantage, have made it the solution of choice among the vast majority of wireless users. As WLANs become more

ubiquitous however, there may develop a resurgent demand for the other two 802.11 Physical Layer specifications as a result of the RF congestion that can be expected from the ongoing boom in wireless communications as well as interference from other devices in the relatively crowded 2.4 GHZ band, such as cordless telephones and microwave ovens.

1. The 802.11B Standard

A contributing factor to the dominance of DSSS in the 802.11 users community is the extension of the original standard known as 802.11b. It specifies the application of Complimentary Code Keying (CCK) modulation, in addition to the original standard's 1 Megabit per second (Mbps) Binary Phase Shift Keying (BPSK) and 2 Mbps Quadrature Phase Shift Keying (QPSK) modulation schemes, to enable increased data exchange rate capabilities of 5.5 Mbps and 11 Mbps.

Actual throughput on WLANs is dependent upon the quality of the communications link between the AP and MU; this is governed by the distance between the two, the number of users associated with the AP and the amount of RF noise in the frequency band of interest. As these parameters increase, the amount of MAC overhead, number of datagram collisions, and lost fragments invariably rise as well, leaving less effective bandwidth for the transmission of content. Hence, 11 Mbps is a maximum design speed. A typical user will not likely see speeds in excess of 6 Mbps except where proprietary (non-802.11 standard compliant) hardware is employed.

2. Other 802.11 Standard Extensions

In addition to 802.11b, which was approved in 1999, two other extensions are poised to take DSSS WLAN

communications to speeds of up to 54 Mbps. The first is 802.11a, which utilizes Orthogonal Frequency Division Multiplexing (OFDM) in the three 5 GHz Unlicensed National Information Infrastructure (UNII) frequency bands. Although the 802.11a extension has (like 802.11b) been an approved IEEE standard since 1999, it has only recently gained FCC approval for use. The second standard extension, 802.11g, has a slightly murkier future. This draft standard is designed to operate on the same channels as 802.11b but the FCC has yet to approve the use of high speed OFDM in the 2.4GHz band. As a result, some manufacturers are shipping hardware that supports an earlier draft version of 802.11g that provides 22 Mbps and is backward compatible with 802.11b. This is a distinct advantage over 802.11a considering the extensive 2.4 GHz WLAN infrastructure that currently exists throughout the United States.

3. 802.11 DSSS Frequency Management

The 802.11 DSSS standard specifies fourteen partially overlapping channels, each 22 MHz wide with center frequencies ranging from 2.412 GHz to 2.483 GHz. In the United States, the FCC has approved use of the lower eleven channels by 802.11b and 802.11g devices. As Figure 2-1 illustrates, the partial overlap between adjacent channels means that no more than three independently operating APs can coexist in the same local area without inflicting partial channel jamming effects on the other APs and their associated clients.

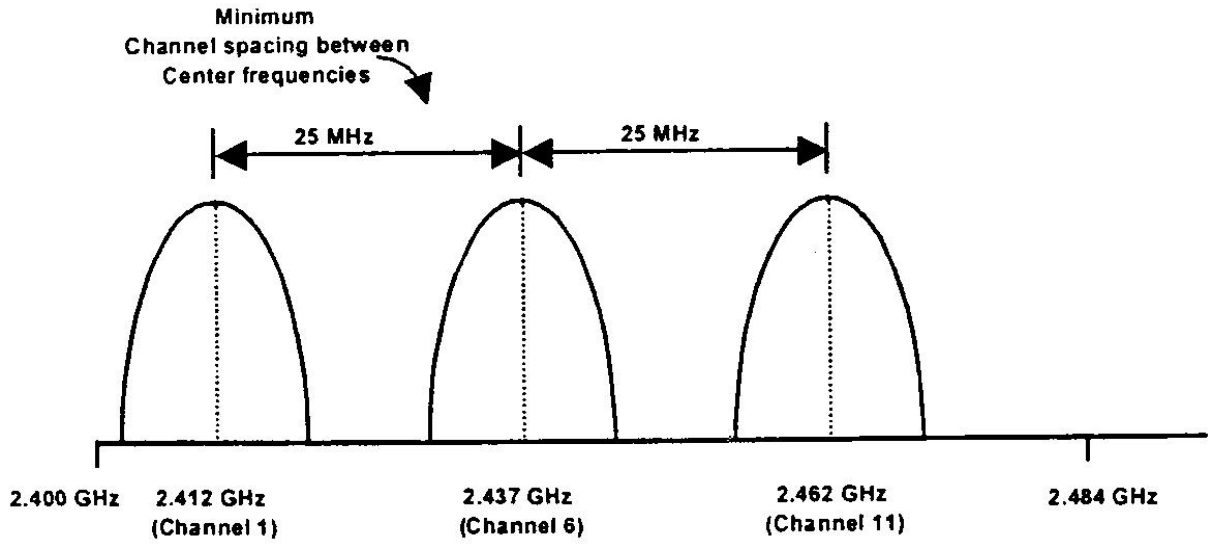

Figure 2.1 Minimum Channel Spacing for 802.11b/g Networks in North America (IEEE 802.11 Handbook, A Designers Companion p. 122)

In contrast, the 802.11a standard is authorized for use over twelve non-overlapping channels, each of them 20 MHz wide. This enables the deployment of twelve independently operating access points with completely overlapping service areas, a considerable advantage over 802.11b installations in high service density environments.

4. 802.11 Throughput Ratings

The 802.11 standard provides for data transfer optimization by means of transfer rate selection for each MU on the basis of the connection quality between two communicating stations. This capability is known as the Dynamic Rate Scaling (DRS).

> [DRS,] as defined by the IEEE 802.11b High Rate standard, always seeks to connect at 11 Mbps, then automatically scales, if network traffic demands, to 5.5, 2, or 1 Mbps for increased signal range. As signal clarity increases, its speed also builds until the system reaches an optimal rate, ensuring the highest level of

service and best continuity for data transmission (http://www.symbol.com/products/wireless/wireless_sp24_11mbps.html)

As may be discerned from the descriptions of the various 802.11 extensions above, each network speed setting is associated with a particular modulation scheme that accounts for the multiple throughput settings at which WLANs may currently operate. For BPSK this is 1 Mbps, for QPSK it is 2 Mbps, for CCK it is 5.5, 11, or 22 Mbps (note that these speeds are perfect multiples of each other), and for OFDM it is 54 Mbps. The means to switch between transmission modes however is handled at the MAC layer.

B. DATA LINK/MAC LAYER

The 802.11 standard for the MAC layer protocol may be best explained as a collection of bit level subfields that reside within byte level fields. These fields comprise the component parts of various 802.11 management, control, and data frames. Frames are in turn the fundamental units of transmitted data passed between stations at the physical layer. This relationship is illustrated in Figure 2.2. The complete systematic assignment of each subfield to a particular task is detailed in the 802.11 Frame Exchange Protocol (FEP), the significance of which is outlined below.

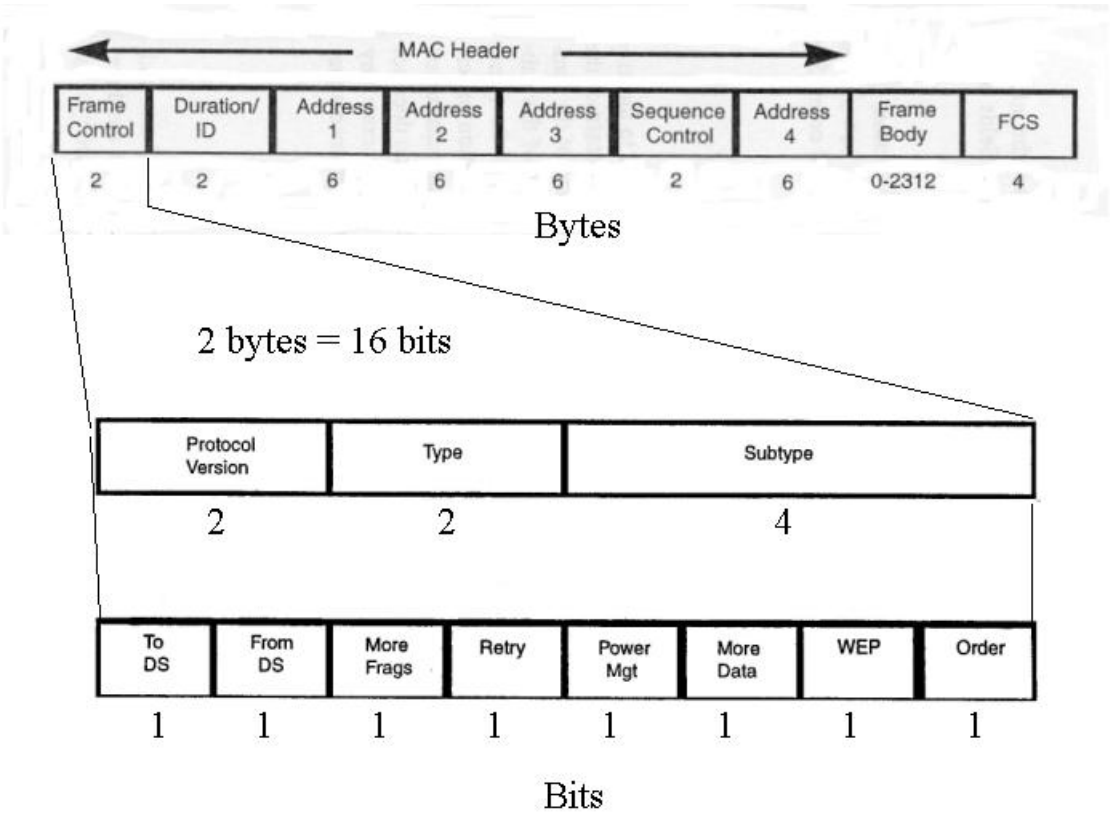

Figure 2.2 IEEE 802.11 Frame, and Frame Control Field Format (adapted from IEEE 802.11 Handbook, A Designers Companion pp. 33, 35)

1. FEP Functionality

The 802.11 standard specifies several measures to alleviate some of the inherent disadvantages of wireless network systems. These are enacted at the MAC layer through FEP mechanisms to combat the problems of data transmission over a shared and unreliable medium.

2. Data Frame Acknowledgement

FEP is employed by both AP and MU devices as a medium reliability countermeasure to speed the process of data exchange confirmation that would otherwise have to been done through higher (and slower) layer mechanisms. Each data frame that passes between 802.11 stations is

automatically acknowledged at the MAC layer by the recipient's network adapter hardware with an acknowledgement frame during a system time interval known as the Network Allocation Vector (NAV). This behavior is central to implementing MU location authentication as will be explained in Chapter IV.

3. Distributed and Point Coordination Functions

FEP is also used to address the "hidden node" problem (illustrated in Figure 2.3) that exists when MUs on opposite edges of an AP service area are unable to receive each other's transmissions. Without some means to deconflict data frame traffic, simultaneous transmissions from multiple MUs vying for AP service would result in data frame collisions requiring the MUs to repeatedly retransmit their frames until they succeeded in delivering their payloads during a confliction free period.

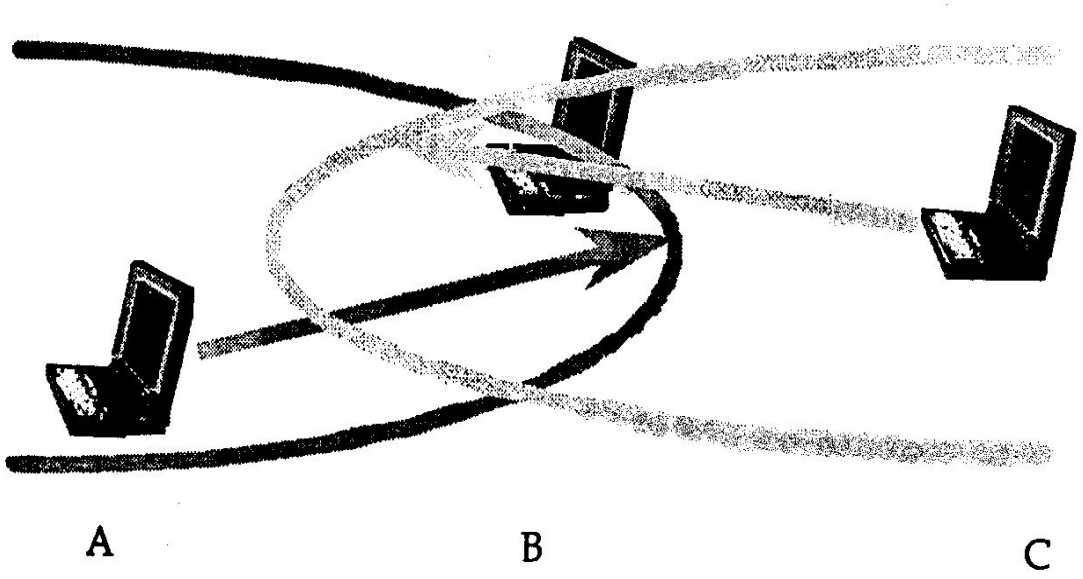

Figure 2.3 The Hidden Node Problem (IEEE 802.11 Handbook, A Designers Companion p. 21)

a. Distributed Coordination Function (DCF)

Because collision detection (as implemented in wired networks) is impractical in a wireless environment, 802.11 depends on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) techniques, also known as “listen before talk” (IEEE 802.11 Handbook, A Designers Companion p. 25) to accomplish efficient data traffic management. FEP utilizes five different Interframe Space (IFS) time intervals as self-regulating mechanisms to reduce the contention period during which stations vie for access to the medium. These are specific to each physical layer implementation of the 802.11 standard (i.e., DSSS, FHSS, and IR) and are the: Short Interframe Space (SIFS), Slot Time, Priority Interframe Space (PIFS), Distributed Interframe Space (DIFS), and Extended Interframe Space (EIFS). Table 1 summarizes the traits of each IFS interval. In addition, Figure 2.4 illustrates the relationship between some of the different IFS intervals.

IFS Unit	Defined by	Duration
SIFS	802.11 standard	10 µsec
Slot Time	802.11 standard	20 µsec
PIFS	SIFS + 1 Slot Time	30 µsec
DIFS	SIFS + 2 Slot Time	50 µsec
EIFS	SIFS+DIFS+ACK based value	364 µsec*
	*calculation of this value is included in Appendix A	

Table 1. DSSS IFS Intervals (adapted from IEEE 802.11b Standard Section 18, Table 101)

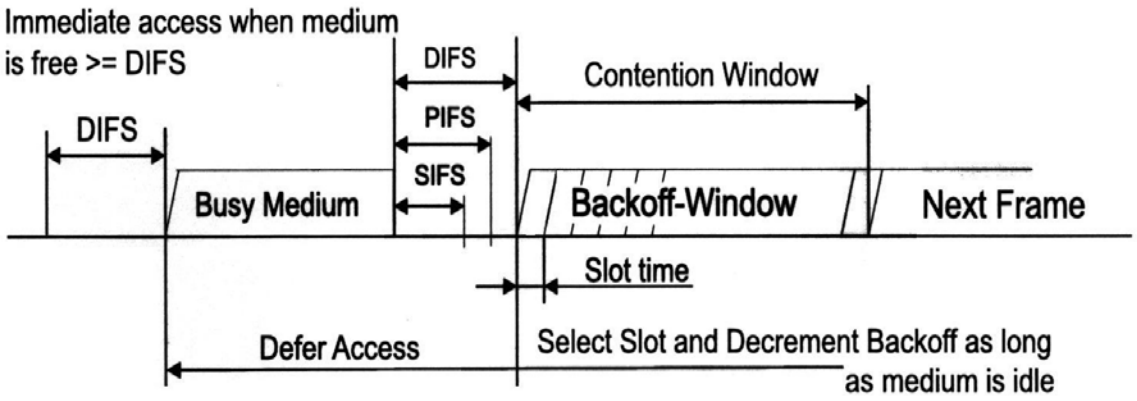

Figure 2.4 Interframe Space Usage (IEEE 802.11 Standard, Section 9.2.3, Figure 49)

The SIFS interval is reserved for receivers to process and transmit MAC layer responses (ACK frames) to incoming data frames. It is designed to ensure that no other station within network reception range attempts to transmit during that time. The DIFS is the base interval upon which all stations build their backoff intervals. If no traffic is detected during the DIFS, the station sends its traffic. On the other hand, if the medium is detected to be in use during the DIFS period, the station adds a random number of slot times to the ongoing DIFS in order to ensure an appropriate offset. At the expiration of the DIFS, the Slot Time counter is decremented for each period during which no traffic is sensed. When the counter reaches zero, the station sends its frame. If an ACK frame is then received, the process begins anew. If not, the binary exponential backoff mechanism is used to double the contention window (starting at 8 minus one, up to a maximum value of 256 minus one) and the process is repeated until the frame is either successfully sent, or is cancelled by a

higher layer time out function. PIFS is a shortened DIFS period that enables an AP to take control of the medium contention process by use of a polling process described below under Distributed Coordination Function (DCF). EIFS is a “last chance” time interval intended to permit stations enough time to respond to correctly received frames whose ACK frames to the originator were lost or corrupted. If an ACK frame is not received within the period of the EIS, the transmitting station repeats its previous transmission until an ACK is received, or a higher layer timeout cancels it.

b. Point Coordination Function (PCF)

PCF is an optional setting complementing the DCF process. It provides a virtual traffic sensing mechanism through a poll and response FEP utility. The PCF makes use of the PIFS to grant an AP control of the medium over stations operating on DIFS interval timers. Participating MUs are permitted to send one frame in response to the AP’s polling frame, which also serves to update the their NAV values. In order to provide service to non-PCF participating MUs, the AP alternates periods of PIFS use with DIFS use. These blocks are termed “contention free period” and “contention period” respectively (IEEE 802.11 Standard, Section 7.1.3.2). Because only properly configured APs are capable of coordinating the polling function, this service is not available in ad hoc (i.e., MU to MU) networks.

c. Request to Send (RTS)/Clear to Send (CTS)

The 802.11 FEP also includes special control frames enabling stations to “reserve” access for incoming traffic in high-density environments or installations with

hidden node issues. These commands are termed Request To Send (RTS) and Clear To Send (CTS). Although the use of RTS/CTS control frames essentially doubles MAC overhead (expanding the two way SEND-ACK exchange between stations to a four way process: RTS-CTS-SEND-ACK), the reduction in frame collisions may actually improve the effective throughput. It is significant to note that RTS-CTS use by the AP is system administrator selectable, but the default setting is off.

4. Wired Equivalent Privacy (WEP)

WEP was incorporated as part of the 802.11 standard in recognition of the fact that simply passing data in the clear over an open shared medium (radio waves) was analogous to conducting a private conversation on the stage of a crowded auditorium. It was intended to provide data security on par with that of a closed system wired network by means of a shared key encryption scheme. WEP encryption is accomplished by applying a cipher algorithm to the body of a data frame resulting in the encryption of the frame's payload and triggering the WEP utilized subfield bit of the Frame Control Field, but leaving the MAC header unaltered. A more specific assessment of WEP's effectiveness as a security measure is included in Chapter III.

C. NETWORK ARCHITECTURE

1. Ad Hoc/Independent Basic Service Set (IBSS) Networks

Informal short-term 802.11 networks are often constructed from free form collections of MUs without any wired connection to a larger network backbone. In IBSS networks, each user must be within direct communications range of the other MUs for a full exchange of data to occur

because there are no devices that are designated to provide relay services from one distant MU to another.

2. Infrastructure/Basic Service Set (BSS) Networks

BSS networks are constructed around an AP that usually provides a wired connection to some larger network infrastructure. Each MU only communicates directly with the AP. The AP is tasked with providing distribution services to its client MUs. Thus, regardless of the distance between MUs, communications between any of them must be relayed through the AP,

3. Extended Service Set (ESS) Networks

ESS networks are installations characterized by multiple APs (tuned to the same channel) with overlapping coverage. The distribution services of ESS APs include cooperative engagement to forward data frames from MUs associated with other APs in the ESS to MUs in their own BSS. This makes the ESS appear to external network entities as though it was one large stationary subnet. In addition, The APs also control seamless handoffs from one AP to another within the ESS to ensure transparent roaming for the MU within the overall coverage area.

D. NETWORK CONNECTION PROCESS

The interaction between stations in establishing a network connection is conducted in four phases. As shown in Figure 2.4, an MU can occupy one of three different states that define its relationship with an AP. The process whereby an MU moves sequentially from one state to the next follows:

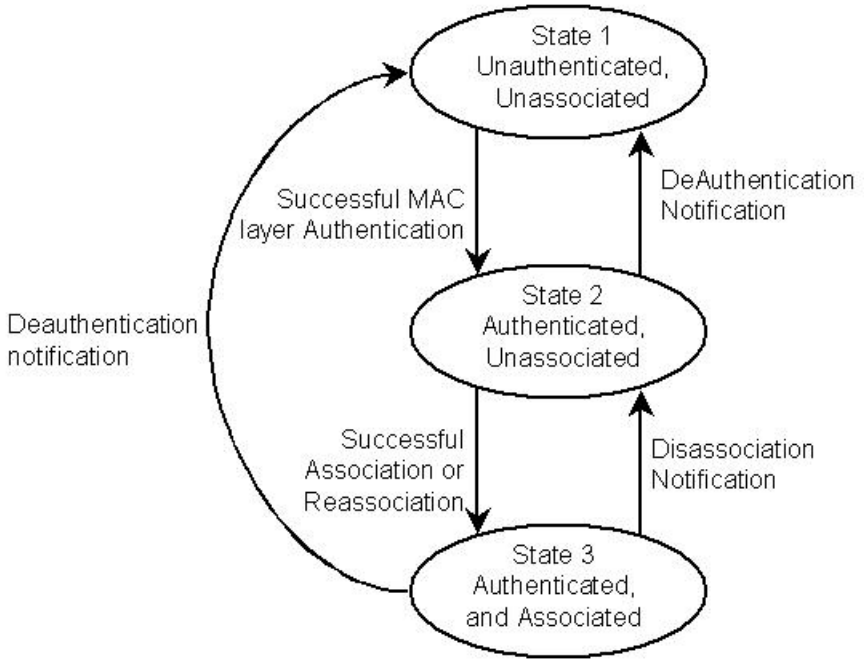

Figure 2.5 Connection States and Services (Adapted from IEEE 802.11 Handbook, A Designers Companion p. 16)

1. State One: Unauthenticated and Unassociated

From an initially unauthenticated and unassociated state, the MU will perform the first two steps toward establishing a client relationship with the AP: Scanning and Synchronization. If the MU is joining an ad hoc network however, it does not move beyond this state. Ad hoc networks do not form complete association connections because they lack any mechanism to regulate traffic amongst the participating MUs.

a. Scanning

Scanning is the process in which an MU seeks out other MUs or APs to form connections. It can be done either actively, where the MU transmits a probe request management frame in order to elicit a response from other stations; or passively, merely listening for a beacon management frame, which may be broadcast by APs in order to facilitate network connections.

b. Synchronization

Synchronization is accomplished by means of periodic beacon management frames that establish and update a common network time reference in order to support the IFS functions that minimize data frame collisions. This function is performed by the AP in an Infrastructure BSS, but shared among all MUs in an ad hoc BSS. Upon completion of this step the MU can begin passing data frames

2. State Two: Authentication

Authentication is the process of one station validating the identity of another. If a WEP enabled connection is to be utilized, it is initiated through the appropriate WEP challenge-response exchange. If open system authentication is used, the AP delivers an authentication valid reply to any authentication request frame.

3. State Three: Association

Association is the final stage in the process linking an MU to an AP. Although an MU may be simultaneously authenticated with numerous APs, it can be associated with only one AP at a time. This prevents confusion in determining which AP provides service in an EBSS environment.

As depicted in Figure 2.4 above, the use of deauthentication and disassociation management frames enables an AP to downgrade the connection state of one or more MUs. This was designed to facilitate data relay and service hand offs to other APs in EBSS network environments, but could also play an important role in enforcing a selective access policy such as location authentication.

THIS PAGE INTENTIONALLY LEFT BLANK

III. WIRELESS LAN SECURITY

> The problem with the 802.11 standard in its current configuration according to network security author Bruce Schneier is that the security protocols fail to achieve their intended objective. "They are not only insecure; they are robustly insecure. The insecurity is woven into the fabric of the wireless protocol, which makes it much harder to fix." (http://www.cioinsight.com/article2/0,3959,394702,00.asp)

A general understanding of current security measures, as they are applied to IEEE 802.11 networks, is useful to understanding the persistent MU authentication vulnerability that location authentication could potentially mitigate. The following paragraphs provide a brief summary of existing wireless LAN security measures and their shortcomings.

A. EMBEDDED 802.11 SECURITY MEASURES

There are a number of network techniques that depend on some facet of the 802.11 specifications, or hardware manufacturers' implementation of the standard, to provide a measure of protection to WLANs. Their collective inadequacies however, should not be considered a reflection of poor system design but rather a number of conscious tradeoffs made to enhance the utility of WLANS for normal MUs.

1. Wired Equivalent Privacy (WEP)

As explained in Chapter II, WEP is the primary security mechanism incorporated into the 802.11 standard to counter the hazards of passing data in the clear over an open shared medium. It has the benefit of being a reasonably strong encryption scheme (provided its shared

key is rotated on a frequent basis) while still being legal to export overseas from the U.S. It is self-synchronizing, which allows for the loss of individual data frames without requiring reinitialization; and it can be efficiently implemented in either hardware of software. (Barnes, P. 203)

The main problem with WEP as it is carried out in 802.11 is that it reuses the 24-bit Initialization Vector (IV) that is combined with a pseudo random number to construct its secret key. Because the IV is relatively short, and is transmitted in the clear as part of each data frame's MAC layer protocol, it will be repeated with sufficient frequency that the rest of cipher can be relatively easily cracked. By collecting a grouping of similar frames (such as TCP exchanges, which utilize identical formatting fields for every frame) that have used the same secret key and IV, enough correlating data can be compared to reveal the secret key. Most of the first generation of WEP cracking programs, such as AirSnort (available at www.Shmoo.com), depends on this approach. Additional technical shortcomings in the 802.11 implementation of WEP also continue to be brought to light; these include: flaws in the state table used to generate the first 256 bytes of WEP cipher stream; vulnerability to cryptanalytic attack based on a comparison of the encrypted version of a known message (intercepted along with the WEP IV through passive sniffing) to repetitive IV based encryption combinations of the known text; and finally, the possibility of inflicting undetected corruption on the data in transit by manipulating the cipher text in special ways that do not change its built-in cyclic redundancy checks.

The fact that WEP's use is optional, however, is considered by many to be its most glaring flaw because it depends on users to actively coordinate its incorporation into their WLANS. When security depends on the novice MU or harried network administrator to carry out additional steps beyond those required to establish connectivity, it often falls by the wayside. As Information Security Magazine contends, actual WEP utilization rates (only 18 of 163 APs in one Boston neighborhood) are probably well below the reported 30 to 40 percent figure that is often reported in industry journals. Further compounding this lack of precaution is the fact that a fair percentage of those that do utilize WEP fail to change the well-known default passwords. This leaves intruders an easy path through the WLAN security perimeter without even needing to crack the WEP key.

In summary, while the simple act of properly activating WEP will reduce the chances of one's network being exploited by casual "war drivers," it will obviously not impede a determined intruder.

2. Service Set Identifiers (SSID) and Beacon Frame Control

Recall from Chapter II that APs and MUs send out periodic frames intended to establish and maintain connections within their BSS. One popular misconception holds that an open system can afford itself some level of privacy by omitting the network SSID from the AP's beacon frames, ceasing to broadcast its beacon frame altogether, or even setting the AP to ignore all MU probe frames not specifically addressed to its SSID. There are two problems with any of these approaches however. The first is that

these actions violate the Wireless Ethernet Compatibility Alliance (WECA) standards colloquially known as “Wi-Fi.” These standards ensure devices not employing active scanning are still able to make network connections. More important (from a security perspective) however, is that the WLAN’s SSID is broadcast in the clear as part of the association process, so potential intruders sniffing traffic in the service area are able to obtain the network’s SSID despite the administrator’s efforts to withhold it.

3. MAC Access Control Lists (ACL)

Just as with wired LANs, WLANs can employ ACLs to define a group of users that are authorized access to the network. If an MU whose unique MAC address is not on the ACL of the particular AP with whom the MU is attempting to establish an association, the connection will be denied. Unlike wired LANs however, the ACL for an AP must include both the SSID (which has no equivalent in wired LANs) as well as the client MAC address. WLAN MAC ACLs are particularly vulnerable to MAC spoofing because their two components are passed in the clear. The AP’s SSID can be easily sniffed as explained above, and the MAC address of legitimate users may be similarly obtained from each frame that is passed between AP and MU. It is a trivial modification to the WLAN adapter client utility that is installed with the MU hardware to change the MAC address of the MU to one that is known to be accepted by the target AP’s ACL. A further disadvantage of WLAN ACLs is the administrative expense to maintain them, particularly if the WLAN in question is subject to a high user turnover

rate. Hence, ACLs are of very marginal use as a security measure in WLAN environments.

4. Immunity to Session Hijacking

Because the 802.11 protocol is designed to be used in a noisy, shared medium, each MU forms an association with only one AP at a time. This exclusive relationship prevents outsiders from inserting themselves into the connection between AP and MU (as in the classic "man in the middle attack") but the MU is vulnerable to spoofed disassociation or de-authentication notification frames from attackers posing as the AP.

Another danger is that of the so-called "rogue AP." Because the 802.11 protocol is designed to operate in noisy RF environments, MUs will form an association with whatever AP meets their connection parameters and has the strongest signal. Hence, an attacker may circumvent an MU's normal connection to its AP by simply presenting a stronger beacon signal through the use of directional antennas and/or RF amplifiers. Once the rogue AP has established a connection with a legitimate MU, it can extract additional network information (such as WEP keys, user names, and passwords) or go after files resident on the MU itself.

5. Transmitter Power Levels and Connection Speed Settings

As explained in Chapter II, the 802.11b standard provides for data link speeds of between 1 and 11 Mbps. DRS will determine the speed at which the MU will connect to the AP as a function of signal strength. The DRS mechanism can be manually overridden however, by specifying a particular connection speed in the device's configuration

utility program. If not set to “automatic”, the station can connect only at the specified speed, or not at all.

Most 802.11 devices are also capable of adjusting their output levels as a power conservation measure. Although the FCC authorizes up to 1000 mW of effective radiated power in the U.S., manufacturers have built their transmitters to operate at a maximum of only 100 mW to ensure their exportability to other more restrictive nations. Hence, available power settings range from the transmitter maximum to as little as 1 mW.

The significance of these two features is that selecting a low AP transmission power setting coupled with the maximum supported data link speed can enable a crude form of range control over the WLAN service area. Although it would force most users to be within a dramatically reduced service area (over which the network administrator can exert more effective physical control), the WLAN would still be vulnerable to intruders with high gain directional antennas connected to their MU devices. The only disadvantage to this approach is that it increases the range at which rogue APs can seduce WLAN MUs away from their network AP on the basis of its greater signal strength compared to the legitimate AP.

6. Network Implementation and Physical Security

The final category of embedded 802.11 security concerns the tremendous flexibility the administrator has in its installation. A meticulous site survey is the key to determining the optimal configuration for a WLAN. By investigating the unique RF propagation characteristics of the installation site, the administrator can employ a

combination transmitter of power tuning and antenna selections to ensure that both service area coverage gaps and unintended bleed-over are minimized. Although omni-directional antennas are by far the most common, an AP can be just as easily deployed with a directional antenna. The primary advantage to using directional antennas is that they provide extended range service in the direction of their gain axis while reducing it elsewhere. Figure 3.1 below illustrates how a combination of antenna types can be used to provide total service area coverage.

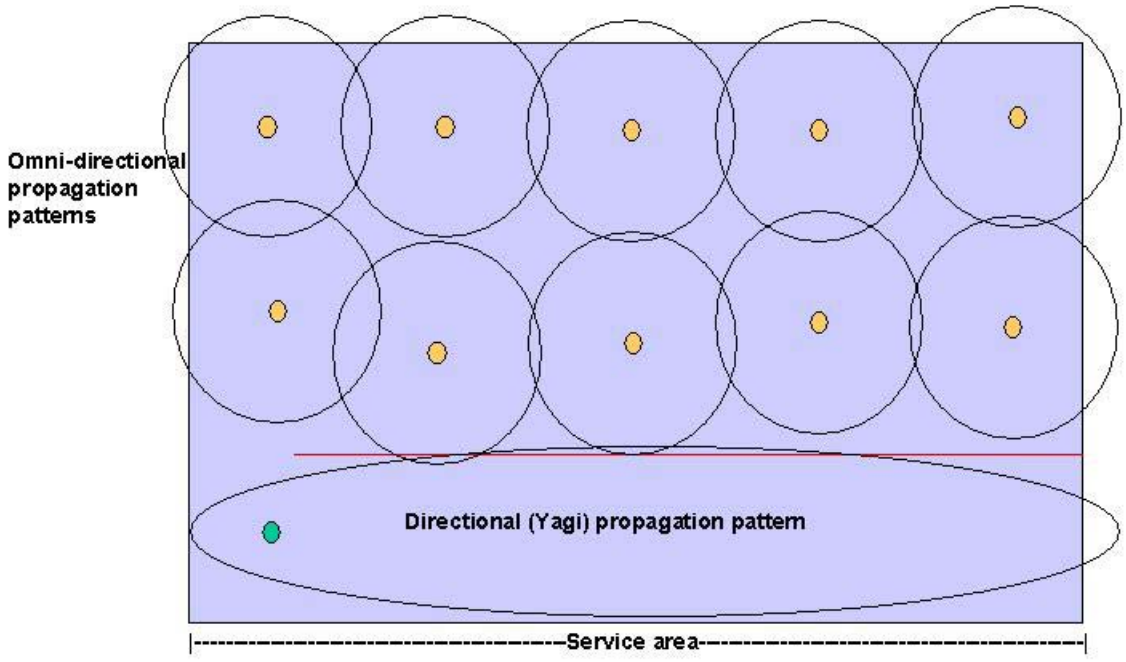

Figure 3.1 Sample Network Antenna Placement (Jim Geier Presentation)

APs are light and compact. Their RF signal penetrates ordinary building materials, and they require no additional

wiring beyond a means to supply their power. This enables their installation in inconspicuous or physically inaccessible locations that prevent tampering. The Achilles heel of the WLAN however, is (predictably) the MU device. Although the 802.11 standard itself has numerous security weaknesses, these can be at least partially offset by a vigilant network administrator. Ensuring proper MU configuration and physical security among the community of users the WLAN serves, can be a far greater challenge. The remainder of this chapter is devoted to a brief description of some of the commercial security models currently being applied as add on services to the 802.11 protocol in order to ameliorate its security vulnerabilities.

B. REMOTE ACCESS DIAL-IN USER SERVICE (RADIUS) AND 802.1X

The IEEE is developing 802.1x as a standard for authentication for both wired and wireless LAN installations. The process is illustrated in Figure 3.2 below. In step one, the MU requests authentication through the AP. The AP responds to probe requests and executes synchronization but holds connection authentication in abeyance until server authentication is complete. In step two, the AP forwards the MU's encrypted credentials to the Authentication Server (AS) such as RADIUS, which allows multiple MUs "to share the same authentication database. This provides a central point of management for all remote network access." (Brenton P.350) In the third step, the AS validates the user's password against its access database and access clearance is sent back to the AP. If the validation fails, the connection is terminated by the AP. Step four involves the activation of the AP port, the exchange of encrypted WEP keys, and full association with

the AP. Finally in step five the MU is permitted access to general network and file servers.

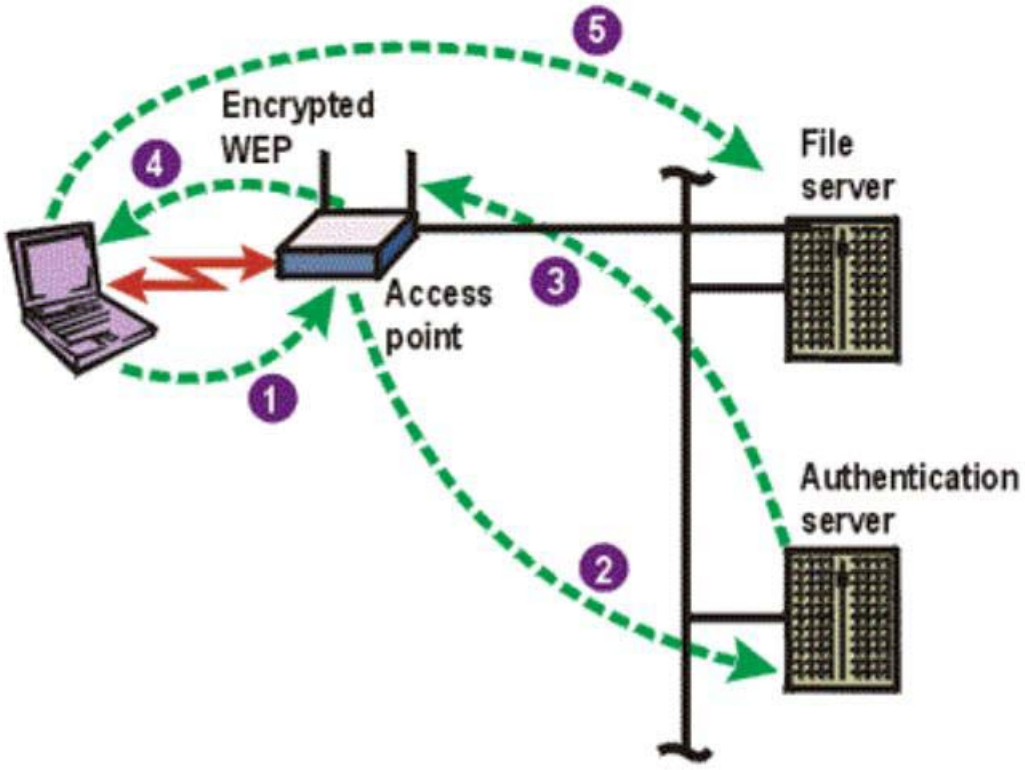

Figure 3.2 802.1x Authentication (Jim Geier Presentation)

There are two main drawbacks to the 802.1x model. The first is that the authentication database is in a single location that, if compromised, would leave the WLAN exposed. The second is that it does not provide complete network protection because it only addresses the need for MU authentication. If used alone, the WLAN will suffer the same deficiencies in confidentiality as an ordinary WLAN because it must rely on WEP to encrypt the data frames being exchanged.

C. VIRTUAL PRIVATE NETWORKS (VPN) AND INTERNET PROTOCOL SECURITY (IPSEC)

VPNs enable MUs to establish secure connections to a private network through an un-trusted medium, typically employing the IEEE defined IPSec protocol as their security mechanism. They also compliment the security of an authentication only scheme, such as RADIUS. As illustrated in Figure 3.3 below, VPN servers are integrated into the wired backbone of the WLAN in order to provide end-to-end security of the exchanged data frames exclusively through the VPN link itself.

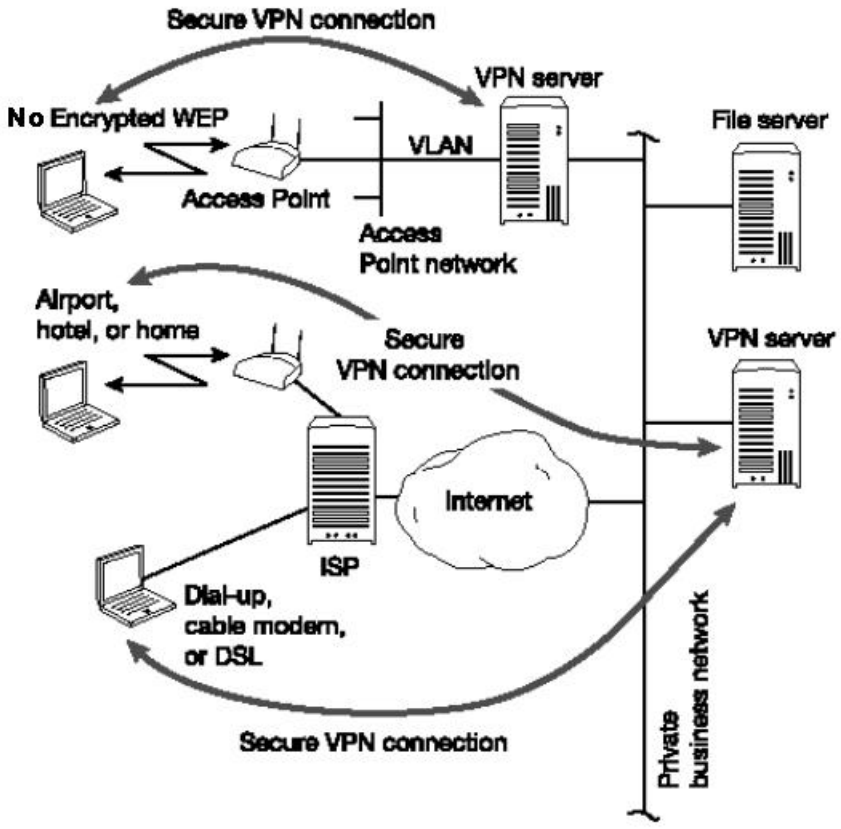

Figure 3.3 VPN Security for 802.11 WLANS (Intel White Paper)

WEP is safely taken out of the communications link by virtue of three distinct security elements provided by

IPSec over the VPN connection. The first is the addition of authentication information to the IP header, preventing access by unauthorized stations or alteration of the data while en route. The second is the bulk encryption of part of the authentication header and the entire data payload using a shared key formed from any of several different algorithms, thereby ensuring confidentiality of the data frames. Finally, there is the internet key management protocol that permits secure exchange of updated VPN shared keys to all MUs over the VPN connection itself, through the use of a separate public-private key set.

The disadvantages of VPNs are in the additional cost required to add them to each network installation, the bandwidth that is consumed by passing each data bit in encrypted form (which decreases the number of MU connections that a single AP can support), and the overhead to correctly establish VPN connections between the MUs and each network they are used to access. Misconfigured VPNs can be vulnerable to session hijacking exploits, and protocol analyzers are capable of capturing frames passed over a VLAN connection related to building the VPN session. From this, the attacker may gain users names and passwords for use in a replay attack. (Barnes p. 322)

D. INTRUSION DETECTION SYSTEMS (IDS)

The newest addition to conventional WLAN security is specialized wireless IDS systems. These systems provide early detection of anomalous behavior on the WLAN through the use of medium scanning remote sensors deployed in the vicinity of each AP. The server appliance, illustrated in Figure 3.4, analyzes the service area traffic in real time and is capable of issuing disassociation frames to

potential intruders it identifies through their use of the ISM spectrum (such as excessive scanning or ad hoc network formation) or MAC spoofing (based on a correlation of the MAC address to other unique hardware and personal profile characteristics that identify the authorized user). It can also act against policy violations by legitimate users (such as installation of free agent APs by employees without IT staff approval, or excessive bandwidth use.) They also have advanced logging functions that enable detailed forensic analysis, and perhaps best of all, they give immediate warnings so that administrators can take appropriate measures to identify offenders and take appropriate action.

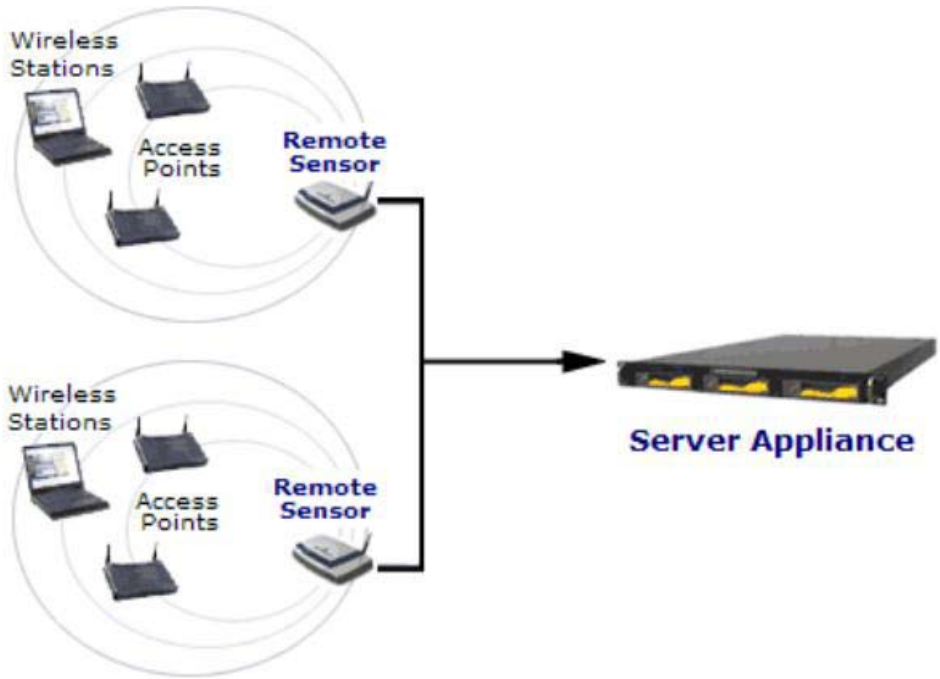

Figure 3.4 WLAN IDS Installation (AirDefense White Paper)

The main weaknesses of IDS systems are that while they are effective at sensing intruders and unauthorized network activity, they are expensive and cannot prevent passive sniffing, or medium flooding by intruders executing Denial of Service attacks.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. LOCATION AUTHENTICATION

A. GPS BASED LOCATION AUTHENTICATION

In 1996, Dorothy Denning and Peter MacDoran introduced the idea of using a Global Positioning Satellite (GPS) based method of absolute Location Authentication (LA) in their security paper: "Location-Based Authentication: Grounding Cyberspace for Better Security." (http://www.cs.georgetown.edu/~denning/infosec/Grounding.txt) The ability of their model to establish location as an independent variable in both wired and wireless network client service has sparked considerable interest in the information security community. As a result, most discussions of LA have focused on the GPS model as their frame of reference. Although the GPS model has excellent potential for many commercial applications, particularly those that transcend a single network location, it cannot be applied without a reliable GPS fix. This requirement restricts its use from many indoor installations (where satellite signal reception is poor) and also means that its use as a primary authentication method leaves the network vulnerable to sophisticated spoofing, or Denial of Service (DoS) through simple jamming techniques.

B. THE SIGNAL STRENGTH ANALYSIS MU LOCALIZATION MODEL

A more recently developed concept in MU localization is based on an analysis of MU signal strength by two (or more) cooperating APs with overlapping service coverage areas. Application of RF propagation loss models to the MU signal strength enables the MU's position to be determined quite accurately in at least two ways. The first is by correlating the MU's current signal strength profile (with

respect to all the APs able to authenticate the MU) to a database that contains a virtual map of the service area expressed in both geo-coordinates and signal strength signatures. The second method illustrated in Figure 4.1 below involves a triangulation of the MU's position by combining the findings of geometrically convenient APs whose range circles are calculated from the received signal strength, a simplified propagation loss model, and an estimate of the MU's signal strength ratio to arrive at a realistic location solution.

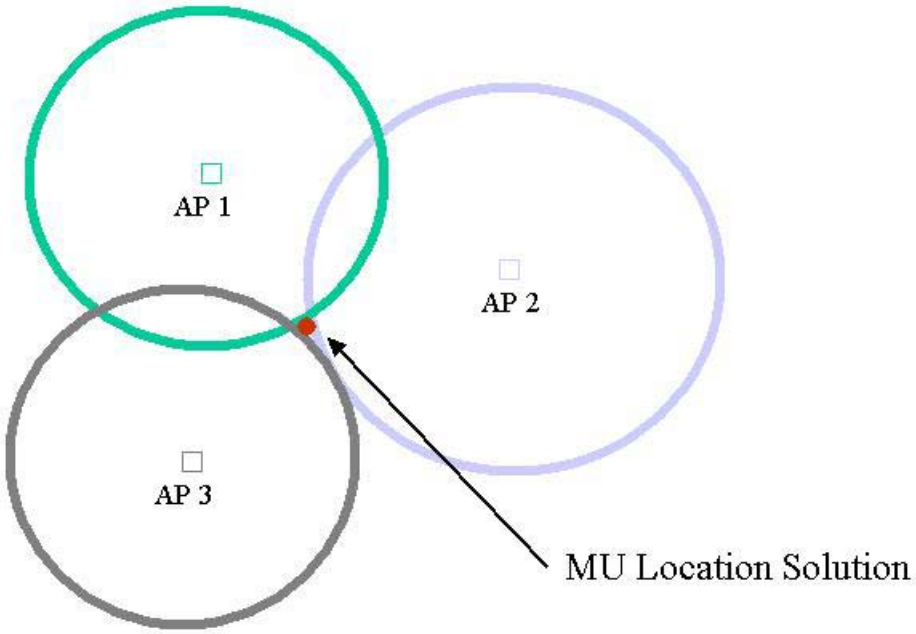

Figure 4.1 Signal Strength Extrapolation Localization

The most significant problem with these approaches is that they require more than one AP to be in contact with the MU. As a result these techniques cannot be scaled

downward for implementation in a single AP installation environments. Another drawback is that if one of the APs is moved, (a capability that is a significant selling point for WLANs,) the MU profile database must be completely recalibrated to ensure accurate results (if they are still possible to obtain). And finally, the requirement for having favorable geometry to effectively triangulate the MU position means that this model is only effective for locating MUs inside the service area. A network intruder utilizing a high gain antenna and/or amplified transmitter outside the intended service area would present more unknowns than the model can accommodate.

C. THE RADAR-BASED MODEL OF LOCATION AUTHENTICATION

As indicated in Chapter I, the intent of this thesis is to explore MU LA as a proof of concept study in a manner that is distinctly different from signal strength analysis or the GPS methods introduced above. It is based on a radar model of localization derived from three unique WLAN attributes described below.

1. Frame Acknowledgement

The first characteristic that makes a radar localization model possible is the 802.11 standard's requirement for network users to acknowledge receipt of each frame that is addressed to them, much like the return of radar pulses off targets within the radar's line of sight and range.

2. NAV Function

A second factor built into the 802.11 standard that enables range finding through simple frame exchanges in a WLAN is the existence of the NAV. As explained in Chapter II, the NAV is a general term for the variable period time

comprised of appropriate SIFS, PIFS, or DIFS, plus backoff-window, that each station incorporates into its network synchronization reference table. The element of randomness incorporated into the NAV as a result of the backoff window is the primary mechanism that facilitates the collision avoidance feature of 802.11's MAC layer CSMA/CA protocol. However it is also updated by every frame a station receives across its antenna. If the frame is not addressed to a particular receiving station, that station's NAV table is incremented by a fixed value contained in the Duration/ID field of the frame's MAC header. This guarantees the frame's addressee a reasonable interval to transmit an ACK frame back to the data frame's originator without the risk of colliding with other traffic.

The significance of this behavior to LA is that because there is no intervening traffic over the WLAN between frame transmission and acknowledgement receipt, the time between these two events can be measuring directly, without having to identify or correlate other signals received by the antenna. In other words, the NAV enables immediate, signature-less RF time of flight calculations at the MAC layer because of protocol collision avoidance and the assumption that the identity of the ACK frame originator is the recipient of AP's last transmission. This behavior is somewhat analogous to the directed beam of a rotating radar transmitter, which only sees returns from targets positioned inside of the transmitter's beam width (rather than its entire search area) at any one time.

It is significant to note that since only stations within communications range of the frame originator perform

NAV updates, the radar model of LA should be more successful when employed on infrastructure networks. The increase in collisions that are likely to occur in ad hoc networks with hidden nodes (when the data frame of one distant MU collides with the ACK frame of another) will make ACK frame latency measurements more difficult.

3. Acknowledgement Frame Delay

The final characteristic of WLANs that complements the radar model is that ACK frames are automatically handled by Wi-Fi compliant hardware at the MAC layer. Because of this, they are generated with a consistent, fixed internal processing delay before being transmitted back to the station that is the data frame's source. The result is that although the response is delayed, it is postponed by a fixed value that can be factored out of the roundtrip time measurement used to establish the station's range, effectively yielding the desired mirror-like target behavior that underlies radar range calculations.

D. TIME OF FLIGHT MEASUREMENTS

The final factor in the radar model of LA is the speed of RF waves through the air. This constant is what allows the direct application of the classic Distance = (Time) X (Speed) equation. Thus, by measuring the latency between the time a frame is transmitted and the time its ACK frame is received, the range between the two communicating stations can be derived from the following equation:

$$R_M = [(T_R - T_T - T_D) \text{ X } (2.997^E8)] / 2$$

Where: R_M is the range between stations in meters
(All time values below are expressed in seconds)

T_R is the time of ACK frame receipt

T_T is the time of data frame transmission

T_D is the time of MU ACK frame generation delay

2.997^E8 is speed of RF waves through air in meters per second

E. RADAR MODEL IMPLEMENTATION CONSIDERATIONS

1. Layer Two Acknowledgement vs. ICMP Ping Response

On the surface, it might appear that a similar range-finding LA technique might be possible by measuring the latency of ICMP Ping commands between two WLAN stations. By simply counting the CPU clock cycles between ping interrogation and reply, it would seem that the range between the two stations should be fairly easily determined. Unfortunately, the interval over which the CPU generates ping replies is slightly variable, resulting in a distribution of values that are spread over too wide a range to be useful. A difference of one microsecond in ping response generation equates to a 150 meter range deviation in the calculated range between stations. The ping method would also be susceptible to range spoofing by intruders capable of reducing their ping response generation delay through the use of faster (or special purpose) processors than the ping originator anticipated.

2. Application to 802.11 Standard Variants

As will become evident in Chapter V, This thesis project was developed and tested utilizing IEEE 802.11b hardware. The principles of radar model LA are valid for any 802.11 compliant format however, and should be completely transferable to 802.11a, 802.11g, and FHSS installations discussed in Chapter II.

F. LA WITHIN THE OVERALL NETWORK SECURITY PICTURE

Properly implemented, LA should be able to provide a spoof resistant method of user characteristic authentication (akin to the current utilization of biometic traits) as the basis for authenticating legitimate WLAN users. It could be used alone, or in conjunction with one (or both) of the other methods in the authentication triad: user knowledge, (usually implemented in software through the use of user names and passwords), and user possessions (such as smart cards, or other tokens that are implemented through hardware devices). It does not require any alteration to MU equipment, and is fully compatible with other security measures such as authentication servers, VPN implementation, and IDS systems explained in Chapter III.

Although LA does not address passive attacks based on eavesdropping, it should provide excellent protection from active network attacks. Its strength lies in its ability to enable an AP to recognize whether or not its MUs are operating from within the perimeter of a pre-defined service area, thereby reducing the physical area over which a WLAN system administrator must be vigilant to a manageable size.

THIS PAGE INTENTIONALLY LEFT BLANK

V. RADAR-BASED LA TEST DESIGN AND RESULTS

This chapter documents a proof of concept study conducted to determine if the range between a host AP and a client MU can be determined using the radar model of LA and off the shelf hardware. By measuring the latency of a series of layer two data acknowledgement control frames sent by and in response to a corresponding series of data frames initiated by an AP, it should be possible to distinguish the reply of a nearby MU from a more distant one. The goal is to accomplish this with sufficient accuracy to be of use in a security application that prevents the formation of AP association beyond a specified range.

A. LOCATION AUTHENTICATION PROOF OF CONCEPT TEST DESIGN

Testing for this location authentication project was performed using two mobile user WLAN adapter cards to form an ad hoc network, the terms Access Point (AP) and Mobile User (MU), as they are described earlier, have been applied for purposes of clarity in distinguishing between the two stations. While the differences between an ad hoc network comprised of two MUs and an infrastructure network formed between a true AP and multiple MUs are not trivial, with the exception of the central time keeping function performed by the AP (discussed below) they are constructively the same.

1. WLAN Hardware

Intersil Corporation’s Prism chipsets are some of the most widely used implementations of 802.11b compliant hardware. They comprise the physical and MAC layer interface for both APs and MUs and are made up of five main

components as depicted in Figure 5.1 below. From antenna to computer interface bus the five integrated circuit chips are: Power Amplifier and Detector, Radio Frequency/Intermediate Frequency Converter and Synthesizer, “I/Q” Baseband Modulator/Demodulator and Synthesizer, Baseband Processor with Rake Receiver and Equalizer, and finally the Medium Access Controller.

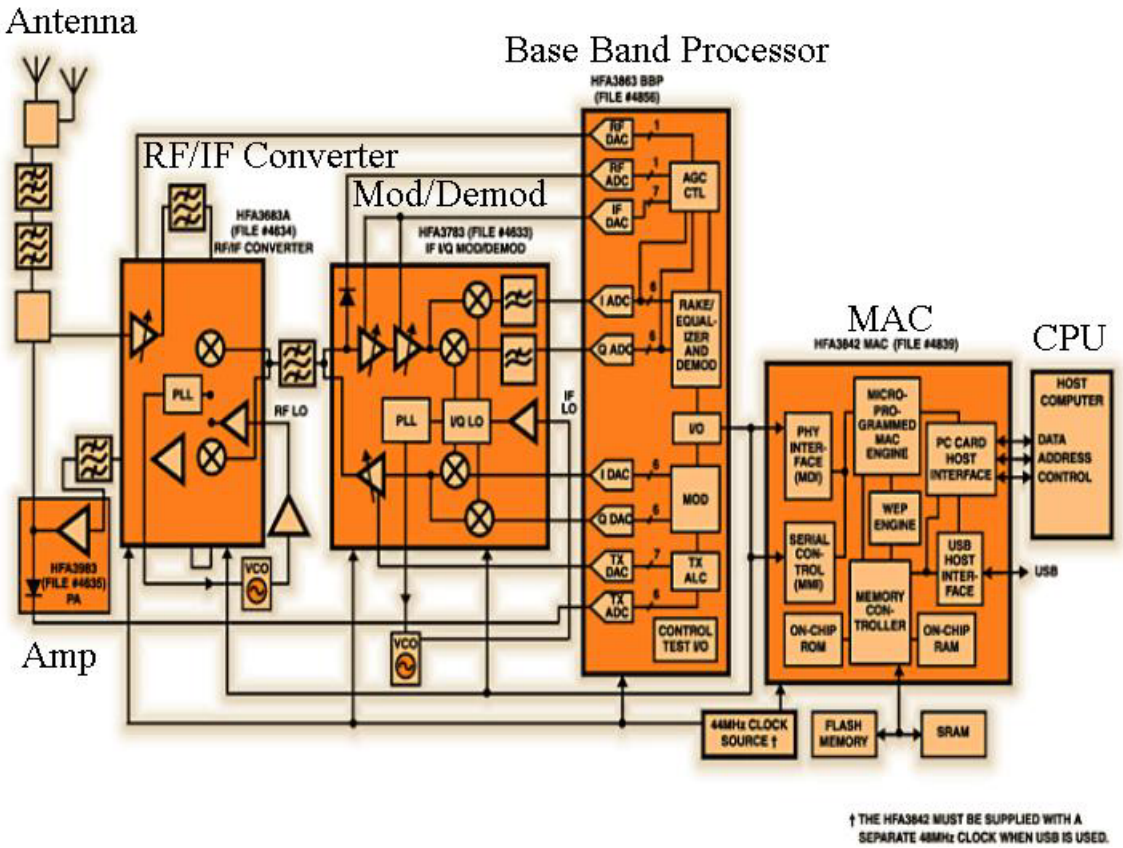

Figure 5.1 Prism 2, 11Mbps Chip Set Overview (http://www.intersil.com/design/prism/ser-pii-11mbps.asp)

Both the Cisco AIR-PCM340 WLAN adapter (used for the MU station) and AIR-PCI350 WLAN adapter (used for the AP) are built from this chip set. The only differences between the two are their maximum transmitted power output (30mW

for the PCM340 vs. 100mW for the PCI350) and physical connection to their host computer. As shown in Figure 5.2 below, the PCM340 connects to the PCMCIA slot of a laptop computer, while the PCI350 connects to a standard desktop computer PCI expansion slot.

PCM340 (PCMCIA)

PCI350 (PCI)

Figure 5.2 WLAN Adapter Interfaces ([http://www.seattlewireless.net/index.cgi/CiscoAironet])

2. Access Point Hardware Modifications

One of the benefits of the radar LA model is that no modifications to the MU are necessary. In order to measure the latency of ACK frames received from the MU in reply to AP data frame transmissions however, appropriate signals from within the AP WLAN adapter chip set must be selected and accessed by our measuring equipment. The object is to extract both transmission pulses and receiver signals in such a way that a unique outbound data frame can be used as the trigger to start a precision timer that would be stopped by the arrival of the corresponding ACK frame. From an inspection of the Prism 2 chipset component pinout diagrams, three appropriate leads (and common ground) were identified on the Baseband Processor chip designated as pins 54, 56, 59, and 61 in Figure 5.3 below.

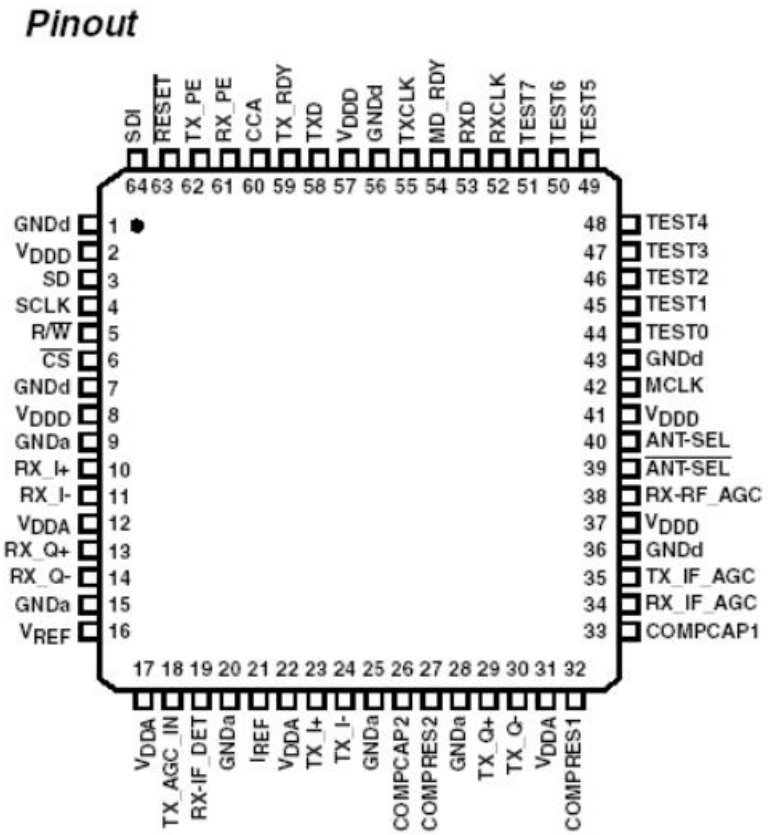

Figure 5.3 Intersil HFA3863 Baseband Processor with Rake Receiver and Equalizer ([http://www.intersil.com/data/fn/fn4/fn4856/fn4856.pdf])

Intersil Corp defines the pins' functions as follows:

Pin 54, MD_RDY is an output signal to the network processor, indicating header data and a data packet are ready to be transferred to the processor. MD_RDY is an active high signal that signals the start of data transfer over the RXD serial bus. MD_RDY goes active when the SFD [start frame delimiter] is detected and returns to its inactive state when RX_PE goes inactive or an error is detected in the header.

Pin 56, GNDd (Digital) DC power supply 2.7–3.6V, ground.

Pin 59, TX_RDY is an output to the external network processor indicating that preamble and

header information has been generated and that the HFA3863 is ready to receive the data packet from the network processor over the TXD serial bus.

Pin 61, (RX_PE) When active, the receiver is configured to be operational, otherwise the receiver is in standby mode. This is an active high input signal. In standby, RX_PE inactive, all RX A/D [analog to digital] converters are disabled.

Accessing the pins required the removal of the chipset card from the PCI adapter housing and cutting through its metal casing to expose the baseband processor chip.

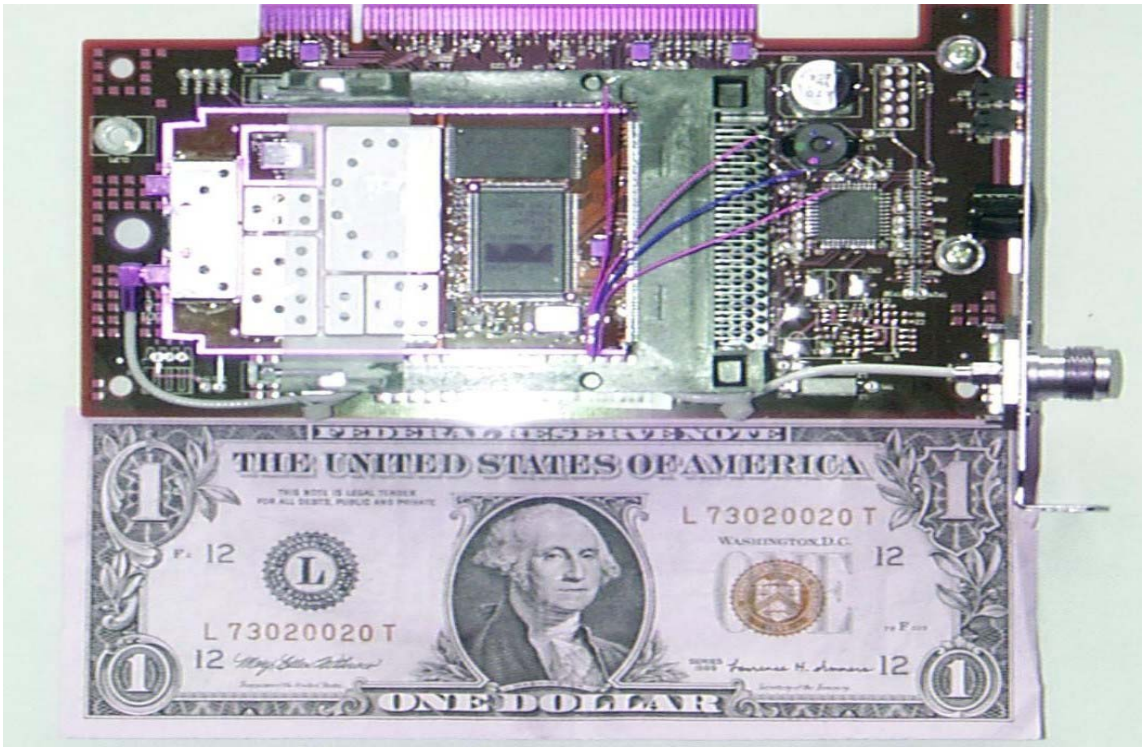

Figure 5.4 Modified AP WLAN Adapter and Size Reference

Electrical leads were micro-soldered to the pins of interest and secured to the edge of the opposite side of the circuit board before replacing the entire card back

into the PCI adapter housing. Figure 5.4 above shows the completed wiring job.

3. Measurement and Data Display Equipment

The two instruments used to gather data from the AP base band processor are shown in Figure 5.5 below.

HP 54510A Digital Oscilloscope

Philips PM6680 Timer/Counter

Figure 5.5 Time Measurement Equipment

While the oscilloscope was very helpful in providing a clear picture of the signal exchange between AP and MU, the timer provided the quickest means of obtaining numerous precision measurements of the time interval between AP antenna events. Figure 5.6 (taken from a three channel oscilloscope) illustrates the relationship between transmission and reception pulses associated with a single data frame transmission utilizing the four-way RTS-CTS-SEND-ACK exchange explained in Chapter II.

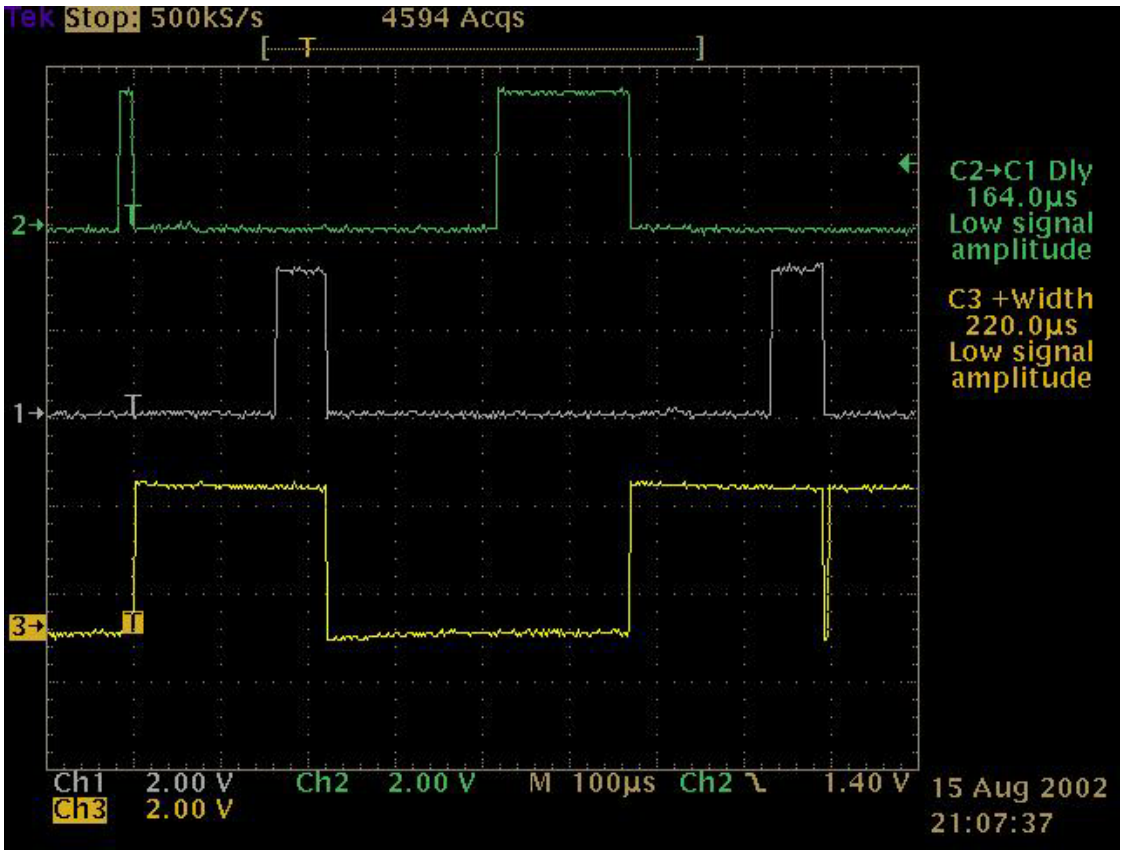

Figure 5.6 Oscilloscope View of Data Frame Exchange

The top trace (Channel 2) depicts outgoing transmission pulses drawn from the baseband processor's TX_RDY (pin 59) signal; the middle trace (Channel 1) displays incoming RF pulses received by the AP from the MD_RDY (pin 54) circuit; and the bottom trace (Channel 3) shows the shift in antenna state (from transmitter to receiver and back again) drawn from the RX_PE (pin 61) connection to the base band processor. As seen in the figure above, the AP to MU frame exchange begins with the AP transmitting an RTS frame. The second significant event is the rise in RX_PE (on Channel 3), which is coincident with the end of the RTS transmission. Next comes the rise in MD_RDY (on Channel One), corresponding to the time at

which the incoming CTS frame is received from the MU. The RX_PE voltage level then drops at the same time as the MD_RDY trace indicating that the incoming CTS frame has ended and the antenna has returned to transmit mode. The cycle is then repeated with the AP's transmission of the data frame and receipt of the ACK frame from the MU.

From a range finding standpoint, the interval of interest runs from the time that TX_RDY falls (denoting the end of the AP transmission) until the rise in MD_RDY (when the incoming MU reply is first detected at the antenna). This value represents the outbound time of flight, plus MU's MAC layer ACK frame generation delay, plus return time of flight. The interval can be measured by subtracting the time value of the falling TX_RDY pulse, marked at some consistent voltage point (the vertical scale value of the signal trace) from the later time value corresponding to the first rise in MD_RDY

4. Network Setup

Establishing the ad hoc network between the AP and MU was a two step process. It was accomplished by first configuring a private Class "C" network on both stations utilizing the Windows LAN connection TCP/IP properties window to assign each station a compatible network address. (The AP's assigned IP address was 192.168.100.100 while the MU was set to 192.168.100.200). The Aironet Client Utility program's "profile manager" was then used to input a unique name, shared SSID, and channel assignment on both stations. WEP was not enabled on the network in order to keep the link between the two stations as clean and simple as possible. Figure 5.7 below shows the AP's settings as summarized in the Client Utility "status" window.

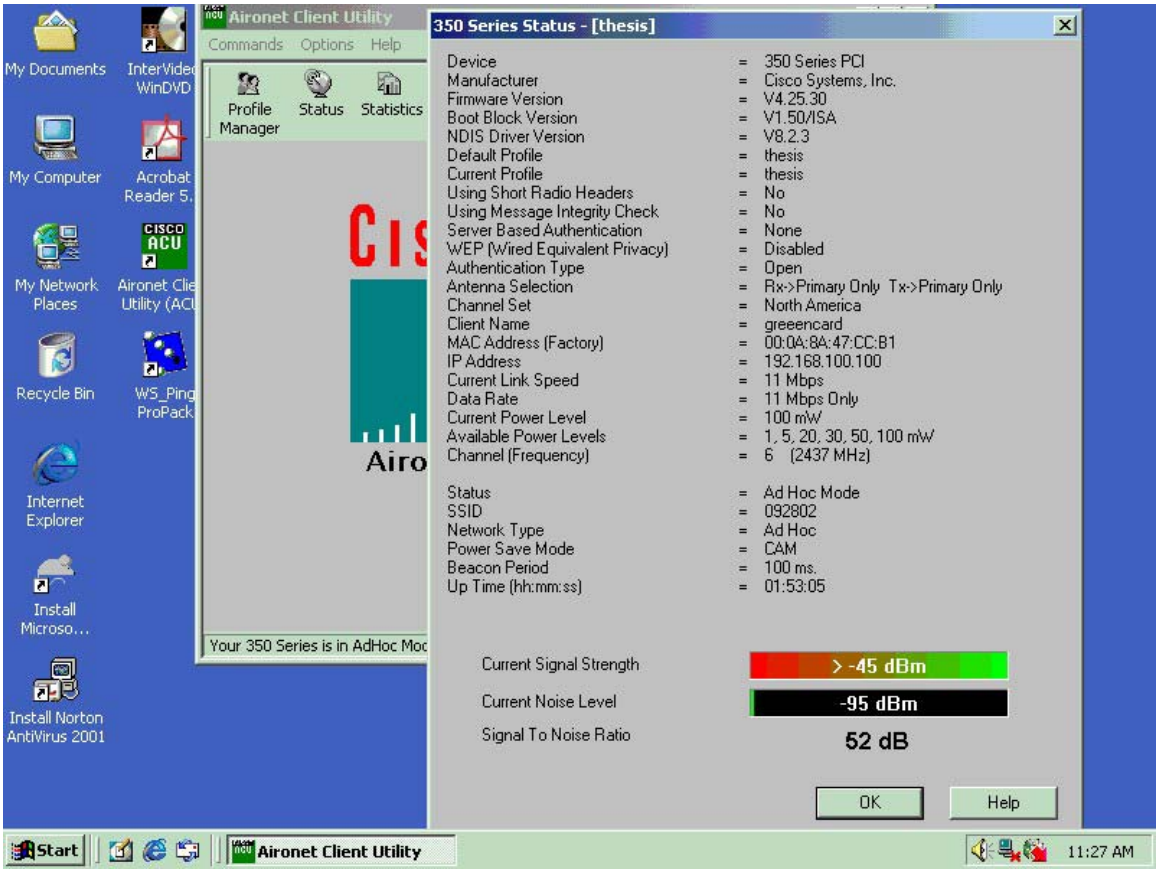

Figure 5.7 AP Configuration Status Display

5. Network Traffic Generation

A steady stream of outbound data frames was highly desirable to facilitate the collection of MU ACK frames during testing. The WS_Ping ProPack utility suite from Ipswitch Corp. provided a convenient means of generating multiple data frames of a fixed size. This made distinguishing outbound data frames from RTS or outgoing ACK frames from the AP (after the ping reply was received from the MU) much easier on the oscilloscope. The graphic user interface for the “Ping” utility is shown in Figure 5.8 below. It shows the IP address of the MU being pinged, the size of the ping packet (in bytes), the ping reply time

in milliseconds (a number far too rough to be of use in MU range finding) and the status of MU reply to each ping.

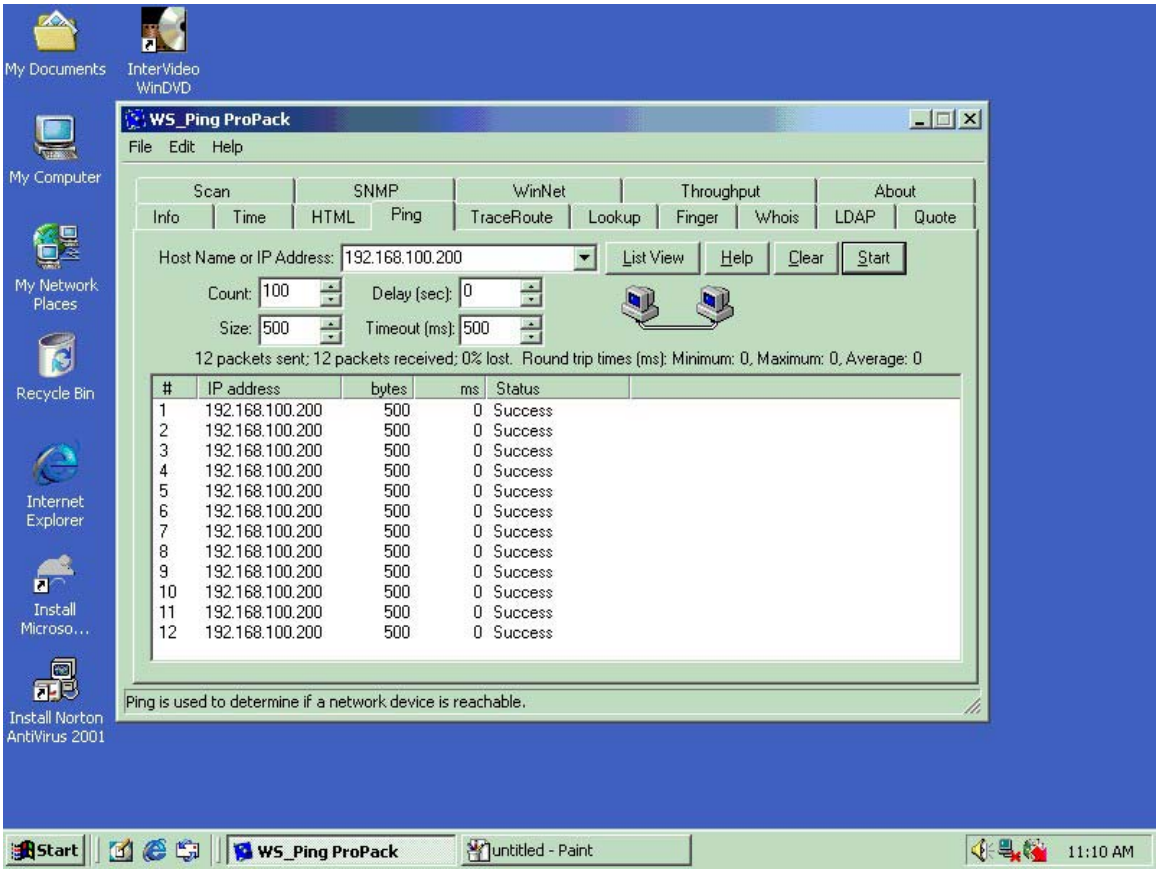

Figure 5.8 WS_Ping ProPack "Ping" Utility Interface

6. Measurement Procedures

The time interval between the end of data frame transmission and MU ACK frame receipt was measured at distances between 0 and 100 meters using both the oscilloscope and timer/counter. Since the radar model assumes a fixed value for the ACK frame generation delay, it was necessary to take zero meter separation measurements to confirm and establish a range of baseline MU Processing Delay (T_D) values. Then, having established a mean zero range ACK frame delay, additional measurements were taken at various distances to see if the increasing ACK frame

delay observed in the data could be statistically correlated to the corresponding increase in AP to MU separation.

The 100 meter maximum distance was selected to ensure that the MU's 30 mW transmitter was within the 11 Mbps outdoor range rating of 120 meters. It was also deemed that since LA is to be used as an intruder prevention measure, the emphasis of the project should be on establishing the minimum resolution that can be achieved in order to support AP access exclusively to nearby MUs.

Measurements taken on the HP 54510A oscilloscope were much slower than those taken with the timer/counter. Consequently, the number of measurements taken at each distance was much lower than when the timer/counter was used. With the oscilloscope it is necessary to capture a single set of frame exchanges by pressing the run/stop button on the instrument. Experience showed that a 200 microsecond trigger delay (with the timebase set at 50 microseconds/division) was the best window to monitor the irregularly appearing frame exchanges. The HP54510A oscilloscope supports linear interpolation up to a factor of 50. In other words, with the timebase set at 50 microseconds/division during trace capture, time difference measurements can be taken at a resolution of 20 nanoseconds by shifting the delay as necessary to keep the trace point of interest on screen while expanding the timebase to 1 microsecond/division

Measurements taken with the timer/counter were gathered by simply pressing the display hold button at random intervals and recording the values of appropriate

measurements that appeared. Because the timer/counter presented a steady stream of noise (apparently random values in the millisecond range) in between valid microsecond measurements, it required patience and multiple attempts to halt the display on a valid data point. The timer/counter was set to trigger the start timer event as the TX_RDY signal dropped through 1.5 volts (just under half the energized voltage level) and stop as the MD_RDY signal rose through the same voltage point. The zero meter T_D measurements established a value of approximately 160 microseconds as the basis for valid measurements.

B. DATA AND ANALYSIS

Figures 5.8 and 5.9 below provide a graphic summary of the data frame transmission completion to MU ACK frame receipt time interval measurements taken via oscilloscope and timer/counter respectively as part of a range-finding field test. The individual measurement values are presented in Appendix B.

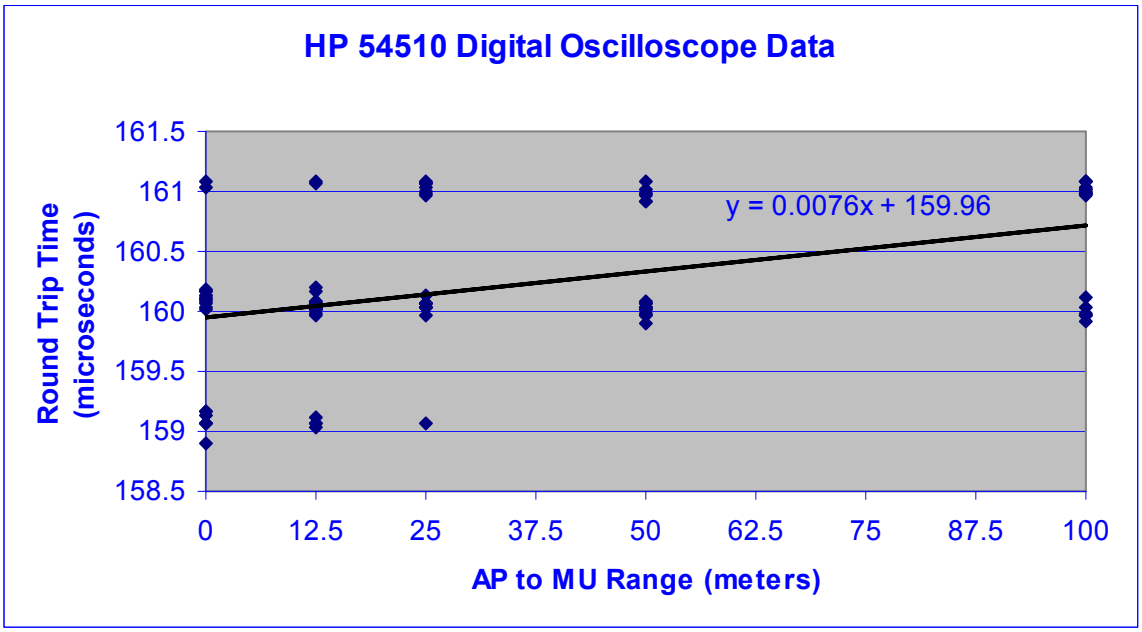

Figure 5.8 Oscilloscope Data Summary

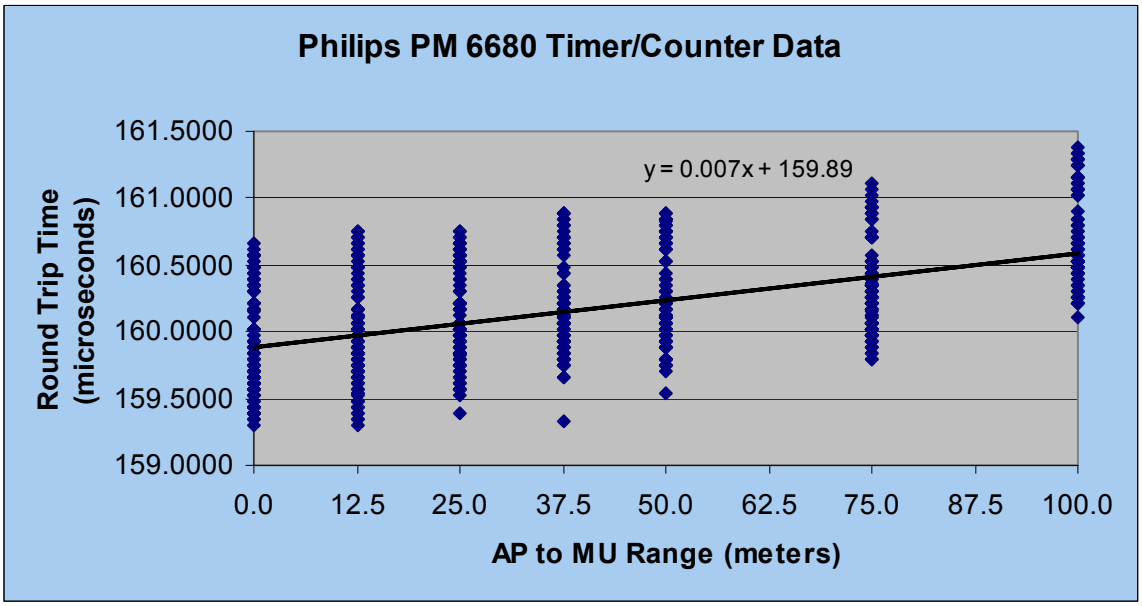

Figure 5.9 Timer/Counter Data Summary

Although the smaller sample size and clustered values of the data points represented in Figure 5.8 (based on 20 measurements for each range value tested) make the relationship between time and distance appear more tenuous than in Figure 5.9 (which is based on 100 measurements per tested range value), the least squares regression lines calculated for each set of data have nearly identical slope values: 7.6± 3.1 nsec/m of range for the oscilloscope data and 7.0± 0.8 nsec/m of range for the timer/counter data with 95% confidence. The actual speed of round trip RF propagation time (6.7 nsec/m of range) falls well within the specified interval for both sets of test data, confirming their validity. We can expect the value of the regression lines to continue to fall closer to the RF propagation speed figure as the number of data samples is increased.

Because there is an overlap in the range of values we expect at the various AP to MU ranges, it is necessary to take multiple measurements to distinguish between any two given range values. Naturally, the number of required measurements is directly related to the desired resolution. For any given degree of certainty, a range resolution of (D), requiring (N) measurements, will require 4(N) measurements to discern a difference between two MUs separated by a reduced distance of (D)/2. This relationship is illustrated in Figure 5.10 below, according to the sample size determination formula:

$$n = (Z^2 \ sigma^2)/e^2 \quad \text{(Berernson, p. 384)}$$

where: n = sample size (number of measurements)

Z = the appropriate number of standard deviations to achieve the desired level of certainty.

$Sigma^2$ = variance of sample data distribution*

e = data sampling error*

* The descriptive statistics report for each set of timer/counter data (in Appendix C) indicate a slight decrease in variance and standard error as range increases. We shall use the highest values observed at any range (0 meters) as a conservative estimate of the population variance and standard error for constructing Figure 5.10, the resolution vs. sampling requirement chart.

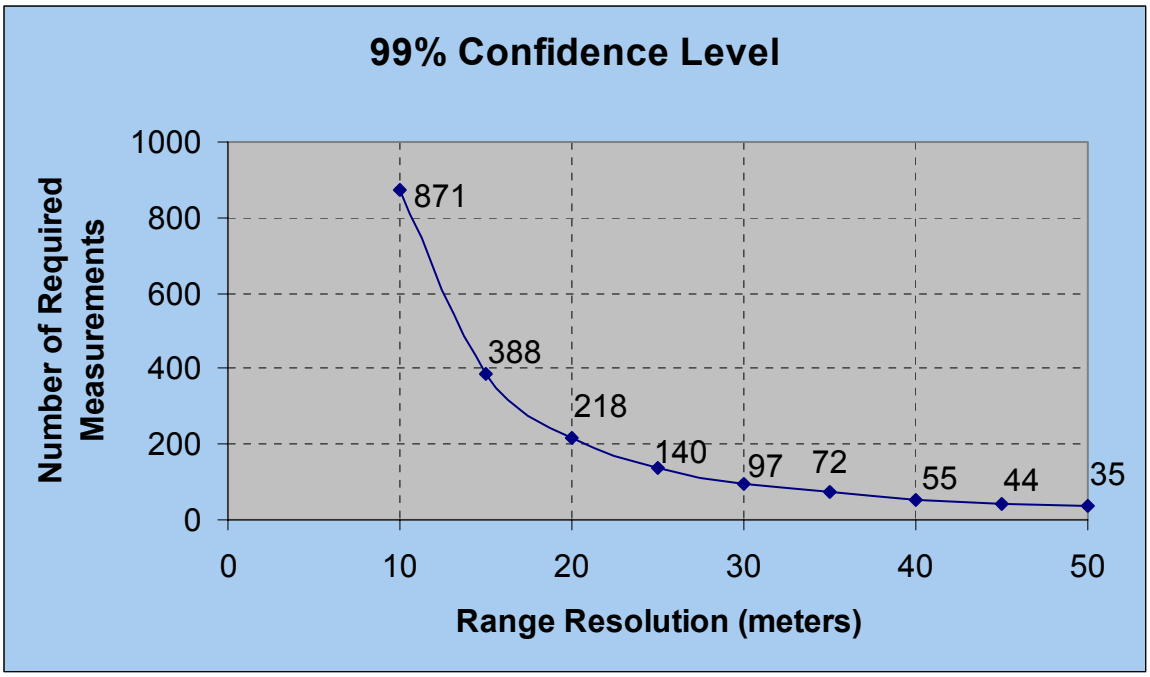

Figure 5.10 LA Resolution vs. Sampling Requirement for Timer/Counter Data

While it may appear that range resolutions beyond 50 meters would require progressively fewer data measurements, it should be noted that the central limit theorem dictates that the number of sample measurements should be kept to at least 30 in order to ensure a reasonably normal distribution about the mean. The relationship between confidence level, range resolution, and sampling requirement can also be depicted for a fixed range resolution value, as in Figure 5.11, reflecting the direct correlation in confidence level to changes in the number of measurements.

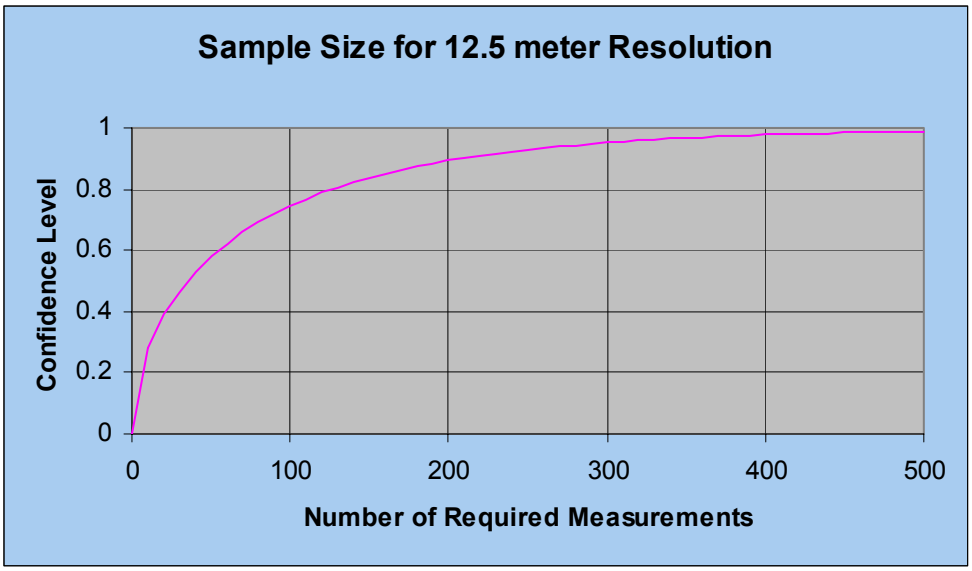

Figure 5.11 Sampling Requirement vs. Confidence Level for Timer/Counter Data

C. MU ACK FRAME GENERATION VARIATION CONSIDERATIONS

From the experimental data sets we see that the variation in data frame transmission to ACK frame receipt is approximately 1.3 to 1.5 microseconds, a relatively large variation compared to the round trip time of flight that we are attempting to measure. Collecting a large number of sample measurements helps smooth this jitter to the point that an average value can be included as part of the fixed MU ACK frame generation delay, but it is important to account for its various components, the sum of which should account for the range of variation seen in the field test measurements summarized above.

1. Time Synchronization Function (TSF) Slippage

Unlike a normal BSS, there is no master time keeper in an 802.11 compliant IBSS (ad hoc) network. Accordingly, "each sta[tion] in an IBSS shall adopt the timing received from any beacon or probe response that has a TSF value

later than its own TSF timer." (IEEE 802.11 Section 11.1.1.2) This can also take place when the synchronization of two communicating stations is adjusted by the duration value contained in the ACK frame. As a result we can expect that there may be an occasional slip of one microsecond (the fundamental unit of TSF timekeeping) between TX_RDY and MD_RDY synchronization during the span of one data frame transmission to ACK receipt by the AP. We should not expect this degree of variation when implementing the radar LA model on a standard BSS.

2. Delay Spreading

Delay spread is associated with multipath signal return and is inversely proportional with data throughput settings. The slower a station expects to communicate with another, the longer it allows for a strong signal to arrive and the more sensitive its receiver setting. As a result, indirect "multipath" signals may arrive that are stronger than the faster direct path signals and become the signal that the receiver actually processes. For the Aironet 350 network adapter the delay spreading value at 11 Mbps is approximately 140 nsec.

3. Signal Arrival to Signal Processing Delay

A small amount of variation in processing delay will also occur due to misalignment of RF signal energy arrival time and the onset of a new baseband clock cycle. If the signal arrives out of sync with the 44 MHz clock that governs MAC layer processing, it will not be processed until the beginning of the next clock cycle. This will produce a jitter of up to 23 nanoseconds for both the outbound data frame at the MU as well as the returning ACK

frame at the AP (for a total jitter range of 0 to 45+ nanoseconds). Transmitter response time is not a contributor to this variation because it remains synchronous with the clock signal and is incorporated as part of the fixed ACK frame generation delay.

4. Measurement Error

The final factor that accounts for some of the range in values observed during testing is simple measurement error. Signal noise in the 2.4 GHz spectrum is likely to have some effect on the measuring equipment timing trigger, introducing a variable amount of jitter to the overall measurements.

D. SUMMARY

This chapter has documented the set up, data collection and analysis of a WLAN location authentication technique intended to enable a modified AP to distinguish the difference between MUs positioned at various ranges from the AP. Although the variation observed in the data was significant, the majority of it can be attributed to the test network’s ad hoc construction. A statistical analysis on the collected data indicates that this proof of concept implementation is fully capable of discerning between two different MUs separated by 10 meters or less, given a sufficient number of data frame exchanges from which measurements can be taken. Implementation in an IBSS should produce a considerably improved resolution.

VI. CONCLUSION AND RECOMMENDATIONS FOR FURTHER STUDY

A. CONCLUSION

This thesis has demonstrated a radar-based model of LA as a potential method of limiting access to WLANs to a specific area of coverage defined by a network administrator. Figure 6.1 below illustrates the three categories a mobile user could fall into as a result of its implementation: The Inner zone termed the “Assured Connectivity Area” is defined by the mean ACK frame generation delay time of participating MUs, plus the round trip time of flight for RF energy between AP and each MU.

The “Ambiguous Connectivity Zone” represents the area in which legitimate clients may be denied service, but intruders might still be able to make illicit connections to the AP. The depth of this zone will be equal to the resolution of the system, and as explained in Chapter V, will be a function of the number of measurements taken by the AP. The outside perimeter of this circular area represents the physical area over which the network must be guarded by other means to prevent the occurrence of insider attacks/intrusions on the AP.

Outside of the Ambiguous Connectivity Zone lie the areas in “Non-Connective Range”. The radar-based LA model is designed to provide protection against network intrusions from wireless users throughout this area.

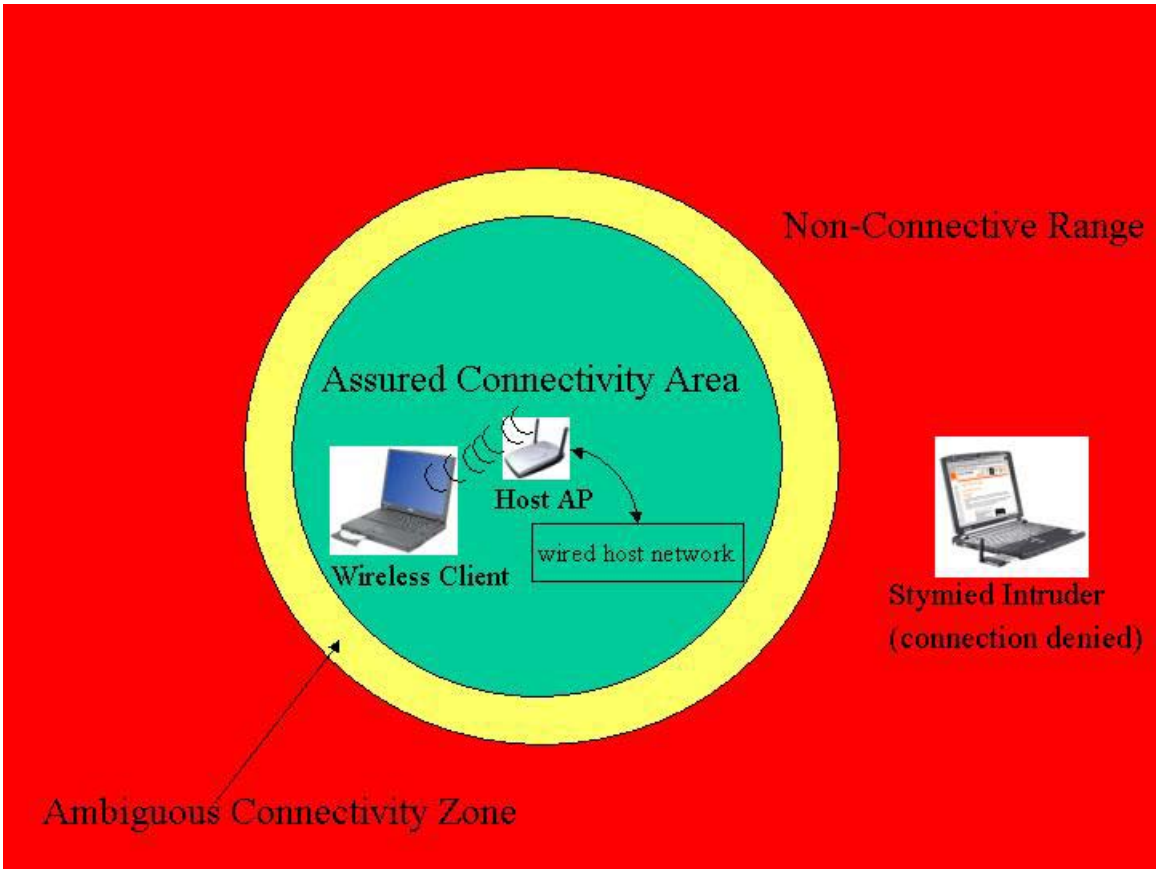

Figure 6.1 Radar-Based Location Authentication Implementation

Implementation of the LA model might make use of a running average of data frame ACK response times to govern connection status. This would enable the system to buffer the service area fringes to avoid unintended disassociations generated by the system's connection enforcement apparatus. It would also prevent an intruder from entering the Assured Connectivity Area to establish an unauthorized connection and then moving outside the service area to exploit it. Obviously the number of measurements that the system would use to govern resolution would also determine the model's response period to an MU's changes in range. The difference in connection time would be marginal

(a matter of seconds) however, since measurements could be taken with every data frame exchange.

B. VULNERABILITIES

1. DOS Attacks

On the surface, it might appear that simply flooding the AP with ACK frames would enable an intruder to satisfy the requirement of answering the data frame almost immediately after a data frame is transmitted. This technique could be easily defeated, however, by instituting a filtering rule that specifies a “no earlier than” window for ACK frame arrival. If an ACK arrives before the baseline ACK generation delay interval has elapsed, the originating MAC could be identified and disassociated. Aligning an ACK frame flood to coincide within the window of permissible values would therefore be extremely difficult to do. ACK frame flooding might create enough confusion to slow or shut down the WLAN communications link between an AP and its MUs, however.

2. Client Spoofing/MAC Sharing

One serious threat to the integrity of LA is the possibility of an intruder using a small wireless device placed inside the Area of Assured Connectivity to provide the required ACK frames for an intruder positioned outside the service area and using the same connection parameters. Countering this possibility would require continued vigilance within the physical footprint of the Area of Assured Connectivity, or other layered network connection protection measure such as VPN.

3. ACK Frame Generation Delay Minimization

Because only one vendor’s hardware was tested during the course of this thesis it remains unknown whether there

may exist other network adapters with shorter ACK frame generation delay. Implementing a zero range value that is too long could allow those with shorter delay cards to falsely appear to be inside the Assured Connectivity Area. The prospects of potential intruders being able to adjust an individual network adapter (either through firmware or hardware alteration) however, is considered remote.

C. OFFENSIVE POTENTIAL FOR RADAR-BASED LA

Network security techniques rarely have a solely offensive or defensive application. Radar-based LA is no exception. In addition to its use as a means to derive the location of MUs, LA could also be used by intruders to refine the position of unprotected APs. Most current AP plotting software associated with wardriving utilities plot a GPS fix at the user's position when a connection to an AP is made (creating a considerable offset error). With LA, the intruder would be able to establish the AP's range from their current location and with the aid of their GPS module, triangulate the AP's exact location from two or three well-positioned range fixes.

D. LIMITATIONS OF STUDY

There are two main limitations of this proof of concept study. The first is that as a layer one security solution there was no embedded method for avoiding the necessity of manual data measurement and sample filtering. The tediousness of collecting a sufficient number of accurate data points to be of use in discriminating between two MU range values can hardly be overstated (especially when performed on the oscilloscope). The second is that the current model is a range-only solution. In order to realize its full potential, the radar model of LA should be

expanded to include an azimuth resolution capability as described below.

E. RECOMMENDATIONS FOR FURTHER STUDY

1. Measurement and Filtering Automation

The most important improvement over the proof of concept implementation of the radar LA model would be the automation of the measurement and filtering functions so that measurements can be taken quickly (and reliably) enough to enable real world application of the model. The most obvious way to accomplish this would to incorporate an internal precision timing and analysis card into the AP computer platform. The supporting software would then be used to control measurement collection, filtering (to eliminate erroneous measurements and spurious noise), and storage. The measurement database would then be compared against a stored profile to ascertain whether the MU's connection should be permitted. If it is not, a disassociate frame would be sent to that particular MU to terminate its connection.

2. Azimuth Resolution

Another logical extension of the radar LA model is to provide a means for establishing the azimuth position of individual MUs. A rotating directional receiver integrated with the AP's omni-directional service area antenna could utilize MU signal strength to establish the MU's position within the antenna's beamwidth (or less if the rotation rate was correlated to the duration of narrow beam connectivity). Once coupled with a range value provided by the exchange of data and ACK frames, an MU's position could be fixed to within a cell defined by the prevailing range and azimuth system resolutions.

3. Graphic User Interface Configuration Manager

Yet another refinement to the implementation of the radar-based LA would be to incorporate a software program to manage the LA functions within one menu. This utility would provide both the means of control and a graphic display of the impact each setting has on the system's function.

4. Cross Vendor Comparison of ACK Frame Generation Delay Values

A comparison of ACK frame generation delay values among all commercially available network adapter cards should be performed to identify the minimum value, and hence provide an LA implementation with the safest (most conservative) T_D value.

5. WLAN Intrusion by MAC Sharing

A study to investigate vulnerability of an LA implementation to an intruder employing MAC sharing would also be a fascinating investigation. It would examine the viability of an intruder to share an authorized user's ACK frame LA by using the same MAC address, or utilizing a hidden device placed inside the Assured Connectivity Area to provide timely ACK frames to the AP (so as to defeat the AP's LA protection) while occupying a position well outside the intended service area.

APPENDIX A. EXTENDED INTERFRAME SPACE VALUE CALCULATION

The IEEE 802.11 standard characterizes the Extended Interframe Space value based on the physical medium being used (e.g. FHSS, infrared, 802.11a, 802.11b) and is defined as follows:

EIFS = aSIFSTime + (8 x ACKSize) + aPreambleLength + aPLCPHeaderLength + aDIFS

Where: ACKSize is the length in bytes, of an ACK frame; and (8 x ACKSize) + aPreambleLength + aPLCPHeaderLength is expressed in microseconds required to transmits at PHY’s lowest mandatory rate (1 Mbps). (IEEE 802.11, section 9.2.10)

From Chapter II, Table 1 we know that SIF and DIFS durations are 10 microseconds and 50 microseconds respectively. The 802.11 standard (802.11 Handbook p.47) specifies an ACK frame as 14 bytes long and the 802.11b standard extension shows the Preamble length to be 144 bits and PLCP header length as 48 bits.

Dividing the bit totals into the 1 Mbps rate and substituting these values back into the original formula results in: 10 + (8 x 14) +144 + 48 +50 = 364 microseconds.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. DATA TRANSMISSION TO ACK FRAME RECEIPT TIME INTERVAL DATA

Oscilloscope Measurements

(in usecs for each separation range):

0.0 meters	12.5	25.0	50.0	100.0
158.900	159.040	159.060	159.900	159.920
159.060	159.060	159.960	159.960	159.960
159.060	159.060	160.040	159.960	159.960
159.060	159.120	160.040	159.980	159.960
159.140	159.960	160.040	160.020	159.980
159.160	159.980	160.040	160.020	160.040
159.160	160.020	160.060	160.040	160.120
160.020	160.020	160.060	160.040	160.960
160.040	160.020	160.060	160.040	160.980
160.060	160.040	160.060	160.060	160.980
160.080	160.040	160.060	160.060	160.980
160.100	160.040	160.140	160.060	160.980
160.100	160.060	160.960	160.080	160.980
160.120	160.060	160.980	160.920	161.000
160.140	160.080	161.000	160.920	161.020
160.160	160.080	161.040	160.960	161.020
160.160	160.160	161.060	160.980	161.040
160.180	160.200	161.060	160.980	161.080
161.040	161.060	161.060	161.020	161.080
161.080	160.634	161.080	161.009	161.080

Timer/Counter Measurements

(in usecs for 0.0 meters separation range):

159.2967	159.5696	159.7058	159.9329	160.3422
159.3421	159.5697	159.7059	159.9329	160.3423
159.3424	159.5699	159.7059	159.9333	160.3426
159.3875	159.5699	159.7060	159.9336	160.3873
159.3875	159.6147	159.7061	159.9338	160.3878
159.3876	159.6149	159.7063	159.9782	160.3880
159.3877	159.6149	159.7509	160.0246	160.4329
159.3878	159.6149	159.7514	160.0247	160.4330
159.3879	159.6151	159.7519	160.0248	160.4789
159.4331	159.6151	159.7520	160.1148	160.4789
159.4331	159.6152	159.7968	160.1599	160.4789
159.4332	159.6601	159.7969	160.1607	160.4791
159.4333	159.6601	159.7969	160.1607	160.5247
159.4334	159.6602	159.8423	160.2058	160.5693
159.4787	159.6604	159.8424	160.2059	160.5696
159.4789	159.6605	159.8430	160.2060	160.5697
159.5238	159.6606	159.8876	160.2967	160.5699
159.5242	159.6609	159.8877	160.2968	160.5700
159.5244	159.6609	159.8880	160.2970	160.6150
159.5693	159.6610	159.8880	160.3421	160.6605

Timer/Counter Measurements

(in usecs for 12.5 meters separation range):

159.2970	159.6604	159.7971	160.0242	160.3430
159.3428	159.6604	159.8422	160.0244	160.3876
159.3429	159.6606	159.8423	160.0245	160.3879
159.3878	159.6608	159.8423	160.0696	160.4336
159.3879	159.7058	159.8424	160.0698	160.4785
159.4331	159.7058	159.8426	160.0699	160.4787
159.4333	159.7060	159.8426	160.0699	160.4788
159.4335	159.7060	159.8427	160.1150	160.5243
159.4785	159.7061	159.8428	160.1151	160.5691
159.4790	159.7061	159.8875	160.1153	160.5693
159.4798	159.7061	159.8878	160.1153	160.5698
159.5240	159.7513	159.8878	160.1605	160.5701
159.5240	159.7514	159.8879	160.1607	160.6150
159.5329	159.7516	159.8880	160.1608	160.6156
159.5343	159.7516	159.9332	160.1610	160.6607
159.5694	159.7518	159.9333	160.2512	160.6608
159.5695	159.7520	159.9337	160.2517	160.7059
159.6151	159.7967	159.9786	160.2970	160.7061
159.6151	159.7969	159.9787	160.3420	160.7519
159.6159	159.7970	160.0240	160.3427	160.7520

Timer/Counter Measurements
(in usecs for 25.0 meters separation range):

159.3880	159.7968	159.9788	160.2059	160.5243
159.5246	159.7969	159.9788	160.2060	160.5244
159.5692	159.8198	159.9788	160.2061	160.5692
159.5693	159.8420	159.9790	160.2061	160.5694
159.5693	159.8422	159.9791	160.2061	160.5697
159.5696	159.8423	160.0239	160.2062	160.5697
159.5699	159.8424	160.0240	160.2063	160.5698
159.6149	159.8426	160.0241	160.2969	160.5699
159.6150	159.8427	160.0242	160.2969	160.6149
159.6153	159.8428	160.0243	160.3428	160.6150
159.6604	159.8878	160.0248	160.3872	160.6151
159.6609	159.8879	160.0691	160.3878	160.6152
159.7060	159.8879	160.0695	160.4334	160.6600
159.7061	159.8879	160.0697	160.4787	160.6603
159.7513	159.9331	160.0700	160.4789	160.6604
159.7513	159.9332	160.1155	160.4789	160.6608
159.7516	159.9334	160.1602	160.5239	160.7060
159.7516	159.9336	160.1604	160.5239	160.7060
159.7518	159.9337	160.1607	160.5241	160.7513
159.7965	159.9787	160.1608	160.5243	160.7516

Timer/Counter Measurements

(in usecs for 37.5 meters separation range):

159.3328	159.8880	160.0694	160.1607	160.5699
159.6605	159.8881	160.0694	160.1608	160.6149
159.6607	159.9330	160.0694	160.2057	160.6151
159.7509	159.9331	160.0695	160.2058	160.6152
159.7513	159.9331	160.0697	160.2059	160.6602
159.7518	159.9331	160.0697	160.2059	160.6605
159.7518	159.9332	160.0697	160.2059	160.6605
159.7967	159.9333	160.0698	160.2063	160.7057
159.7968	159.9334	160.0698	160.2066	160.7059
159.7969	159.9335	160.0699	160.2512	160.7060
159.7969	159.9338	160.1150	160.2514	160.7063
159.7970	159.9785	160.1150	160.2968	160.7515
159.7971	159.9788	160.1151	160.2969	160.7966
159.7972	159.9788	160.1151	160.2970	160.7968
159.8420	159.9790	160.1151	160.2972	160.7968
159.8424	159.9790	160.1154	160.3422	160.8420
159.8426	160.0242	160.1155	160.3429	160.8423
159.8427	160.0243	160.1601	160.4330	160.8875
159.8878	160.0246	160.1605	160.4336	160.8878
159.8879	160.0691	160.1606	160.4787	160.8881

Timer/Counter Measurements

(in usecs for 50.0 meters separation range):

159.5332	159.9331	160.1150	160.2970	160.7062
159.7061	159.9333	160.1150	160.2970	160.7063
159.7512	159.9336	160.1151	160.2973	160.7065
159.7512	159.9338	160.1151	160.3425	160.7511
159.7514	159.9339	160.1151	160.3428	160.7512
159.7514	159.9787	160.1151	160.3873	160.7512
159.7522	159.9789	160.1152	160.3880	160.7515
159.7970	159.9790	160.1152	160.3881	160.7518
159.7970	159.9790	160.1153	160.4334	160.7519
159.7970	160.0240	160.1156	160.5240	160.7969
159.7972	160.0241	160.1157	160.5241	160.7969
159.7972	160.0241	160.1602	160.6151	160.7970
159.7972	160.0242	160.1609	160.6152	160.8247
159.8873	160.0692	160.1609	160.6159	160.8421
159.8876	160.0695	160.1612	160.6602	160.8423
159.8879	160.0698	160.2058	160.6603	160.8423
159.8880	160.0699	160.2059	160.6604	160.8427
159.8881	160.0700	160.2060	160.6607	160.8428
159.8882	160.0701	160.2060	160.7059	160.8880
159.8882	160.1150	160.2512	160.7061	160.8881

Timer/Counter Measurements

(in usecs for 75.0 meters separation range):

159.7966	160.0240	160.1605	160.2970	160.5241
159.7970	160.0240	160.1606	160.2970	160.5246
159.8423	160.0241	160.1607	160.3421	160.5693
159.8425	160.0242	160.1607	160.3422	160.7058
159.8873	160.0243	160.2059	160.3422	160.7060
159.8876	160.0690	160.2059	160.3422	160.7062
159.8877	160.0694	160.2059	160.3423	160.7062
159.9329	160.0696	160.2059	160.3423	160.7518
159.9330	160.0697	160.2061	160.3423	160.8419
159.9331	160.0697	160.2063	160.3650	160.8422
159.9332	160.0697	160.2505	160.3877	160.8877
159.9786	160.0697	160.2511	160.3877	160.8878
159.9786	160.0699	160.2512	160.4331	160.9333
159.9786	160.1149	160.2516	160.4334	160.9334
159.9787	160.1150	160.2516	160.4335	160.9336
159.9788	160.1154	160.2518	160.4784	160.9336
159.9789	160.1154	160.2968	160.4785	160.9787
159.9789	160.1154	160.2968	160.4785	161.0239
160.0239	160.1601	160.2969	160.5239	161.0697
160.0240	160.1605	160.2969	160.5240	161.1150

Timer/Counter Measurements

(in usecs for 100.0 meters separation range):

160.1149	160.4329	160.5239	160.6603	161.0698
160.2058	160.4329	160.5239	160.6605	161.0698
160.2058	160.4329	160.5240	160.6605	161.0698
160.2059	160.4330	160.5241	160.6608	161.1150
160.2063	160.4333	160.5241	160.7057	161.1151
160.2510	160.4334	160.5241	160.7057	161.1599
160.2515	160.4784	160.5241	160.7059	161.1604
160.2515	160.4785	160.5241	160.7059	161.1606
160.2517	160.4785	160.5241	160.7510	161.1607
160.2517	160.4786	160.5242	160.7515	161.1608
160.2518	160.4786	160.5696	160.7966	161.2514
160.2519	160.4787	160.5696	160.7967	161.2517
160.2967	160.4788	160.5697	160.7969	161.2519
160.2968	160.4788	160.5700	160.8420	161.2966
160.2968	160.4789	160.6148	160.8426	161.2967
160.3421	160.4789	160.6149	160.8978	161.2969
160.3425	160.4790	160.6150	161.0238	161.2970
160.3426	160.5239	160.6153	161.0240	161.3422
160.3878	160.5239	160.6601	161.0691	161.3423
160.3879	160.5239	160.6602	161.0698	161.3876

APPENDIX C. DATA TRANSMISSION TO ACK FRAME RECEIPT TIME INTERVAL SUMMARY AND REGRESSION STATISTICS

Oscilloscope Data (in microseconds):

Range 0.0 meters	
Mean	159.841
Standard Error	0.144218219
Median	160.07
Mode	159.06
Standard Deviation	0.644963483
Sample Variance	0.415977895
Kurtosis	-0.591704126
Skewness	0.133410665
Range	2.18
Minimum	158.9
Maximum	161.08
Sum	3196.82
Count	20
Confidence Level(95.0%)	0.301852296

Range 12.5 meters	
Mean	159.959
Standard Error	0.123684446
Median	160.04
Mode	160.04
Standard Deviation	0.553133657
Sample Variance	0.305956842
Kurtosis	0.758865115
Skewness	-0.016086297
Range	2.04
Minimum	159.04
Maximum	161.08
Sum	3199.18
Count	20
Confidence Level(95.0%)	0.2588746

Range 25.0 meters	
Mean	160.393
Standard Error	0.129177764
Median	160.06
Mode	160.06
Standard Deviation	0.577700523
Sample Variance	0.333737895
Kurtosis	-0.510492232
Skewness	-0.222345249
Range	2.02
Minimum	159.06
Maximum	161.08
Sum	3207.86
Count	20
Confidence Level(95.0%)	0.270372252

Range 50.0 meters	
Mean	160.354
Standard Error	0.106029787
Median	160.06
Mode	160.06
Standard Deviation	0.474179624
Sample Variance	0.224846316
Kurtosis	-1.661421072
Skewness	0.669969606
Range	1.18
Minimum	159.9
Maximum	161.08
Sum	3207.08
Count	20
Confidence Level(95.0%)	0.221922964

Range 100.0 meters	
Mean	160.656
Standard Error	0.112461455
Median	160.98
Mode	160.98
Standard Deviation	0.502942918
Sample Variance	0.252951579
Kurtosis	-1.660287529
Skewness	-0.683155744
Range	1.16
Minimum	159.92
Maximum	161.08
Sum	3213.12
Count	20
Confidence Level(95.0%)	0.235384604

Timer/Counter Data (in microseconds):

Range 0.0 meters	
Mean	159.885988
Standard Error	0.038382084
Median	159.7744
Mode	160.4789
Standard Deviation	0.383820844
Sample Variance	0.14731844
Kurtosis	-1.027530686
Skewness	0.467143573
Range	1.3638
Minimum	159.2967
Maximum	160.6605
Sum	15988.5988
Count	100
Confidence Level(95.0%)	0.076158396

Range 12.5 meters	
Mean	159.96037
Standard Error	0.038348545
Median	159.88765
Mode	159.7061
Standard Deviation	0.383485452
Sample Variance	0.147061092
Kurtosis	-0.742811978
Skewness	0.43049948
Range	1.455
Minimum	159.297
Maximum	160.752
Sum	15996.037
Count	100
Confidence Level(95.0%)	0.076091847

Range 25.0 meters	
Mean	160.110794
Standard Error	0.035882734
Median	160.02455
Mode	159.8879
Standard Deviation	0.358827337
Sample Variance	0.128757058
Kurtosis	-1.12101143
Skewness	0.169015565
Range	1.3636
Minimum	159.388
Maximum	160.7516
Sum	16011.0794
Count	100
Confidence Level(95.0%)	0.071199141

Range 37.5 meters	
Mean	160.167735
Standard Error	0.034076097
Median	160.09245
Mode	160.1151
Standard Deviation	0.34076097
Sample Variance	0.116118038
Kurtosis	-0.336684339
Skewness	0.573050723
Range	1.5553
Minimum	159.3328
Maximum	160.8881
Sum	16016.7735
Count	100
Confidence Level(95.0%)	0.067614381

Timer/Counter Data (in microseconds):

Range 50.0 meters	
Mean	160.251461
Standard Error	0.036703864
Median	160.11565
Mode	160.1151
Standard Deviation	0.367038639
Sample Variance	0.134717363
Kurtosis	-1.18991512
Skewness	0.313135367
Range	1.3549
Minimum	159.5332
Maximum	160.8881
Sum	16025.1461
Count	100
Confidence Level(95.0%)	0.072828442

Range 75.0 meters	
Mean	160.29208
Standard Error	0.032483107
Median	160.2284
Mode	160.0697
Standard Deviation	0.32483107
Sample Variance	0.105515224
Kurtosis	-0.096198999
Skewness	0.825403919
Range	1.3184
Minimum	159.7966
Maximum	161.115
Sum	16029.208
Count	100
Confidence Level(95.0%)	0.064453543

Range 100.0 meters	
Mean	160.665119
Standard Error	0.033623282
Median	160.5469
Mode	160.5241
Standard Deviation	0.336232822
Sample Variance	0.113052511
Kurtosis	-0.699235632
Skewness	0.631281936
Range	1.2727
Minimum	160.1149
Maximum	161.3876
Sum	16066.5119
Count	100
Confidence Level(95.0%)	0.066715898

Oscilloscope Regression:

Regression Statistics	
Multiple R	0.435383974
R Square	0.189559205
Adjusted R Square	0.181289401
Standard Error	0.561233736
Observations	100

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	7.22	7.22	22.9218497	5.98071E-06
Residual	98	30.868364	0.314983306		
Total	99	38.088364			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*
Intercept	159.9556	0.081813173	1955.132583	8.6994E-227	159.7932444	160.1179556
X Variable 1	0.0076	0.001587409	4.787676858	5.98071E-06	0.004449839	0.010750161
mean value width +/-	0.003150161					

Timer/Counter regression:

Regression Statistics	
Multiple R	0.537391216
R Square	0.288789319
Adjusted R Square	0.287770393
Standard Error	0.360501193
Observations	700

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	36.83423815	36.83423815	283.4250808	1.2458E-53
Residual	698	90.71285489	0.12996111		
Total	699	127.547093			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*
Intercept	159.8892652	0.022490813	7109.092378	0	159.8451075	159.9334229
X Variable 1	0.007028969	0.000417515	16.83523332	1.2458E-53	0.006209233	0.007848705
mean value width +/-	0.000819736					

APPENDIX D. GLOSSARY OF ACRONYMS

ACK	Acknowledgement
ACL	Access Control List
AP	Access Point
AS	Authentication Server
BPSK	Bi Phase Shift Keying
BSS	Basic Service Set
CCK	Complimentary Code Keying
CPU	Central Processing Unit
CSMA/CA	Collision Sensing Multiple Access with Collision Avoidance
CTF	Clear to Send
DCF	Distributed Coordination Function
DIFS	Distributed Interframe Space
DoS	Denial of Service
DRS	Dynamic Rate Scaling
DSSS	Direct Sequence Spread Spectrum
EIFS	Extended Interframe Space
ESS	Extended Service Set
FCC	Federal Communications Commission
FEP	Frame Exchange Protocol
FHSS	Frequency Hopping Spread Spectrum
GHz	Gigahertz
GPS	Global Positioning Satellite
IBSS	Independent Basic Service Set
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IFS	Interframe Space
IP	Internet Protocol
IPSEC	Internet Protocol Security
IR	Infrared
ISM	Industrial Scientific and Medical
ISO	International Standards Organization
IT	Information Technology
IV	Initialization Vector
LA	Location Authentication

LAN	Local Area Network
MAC	Medium Access Control
Mbps	Megabit per second
MHz	Megahertz
MU	Mobile User
MW	milliwatt
NAV	Network Allocation Vector
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
PCMCIA	Personal Computer Memory Card International Association
PCF	Point Coordination Function
PCI	Peripheral Component Interconnect
PIFS	Priority Interframe Space
QPSK	Quadrature Phase Shift Keying
RADIUS	Remote Access Dial-In User Service
RF	Radio Frequency
RTF	Request to Send
SIFS	Short Interframe Space
SSID	Service Set Identification
TCP	Transmission Control Protocol
TSF	Time Synchronization Function
UNII	Unlicensed National Information Infrastructure
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network

LIST OF REFERENCES

AirDefense, “Wireless LANs: Risks and Defenses,” Alpharetta, GA, AirDefense Inc., 2002.

Akin, Sandler et al., Certified Wireless Network Administrator Official Study Guide. Planet3 Wireless Inc. 2002.

Barnes, Christian et al, Hack Proofing Your Wireless Network, Syngress Publishing, Rockland, MD, 2002.

Berenson, Mark L. and Levine, David M., Basic Business Statistics: Concepts and Applications, 7th edition, Prentice-Hall, Upper Saddle River NJ, 1999.

Cisco Systems Inc., “Cisco Aironet 350 Series Client Adapters Data Sheet.” [http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350c_ds.htm] August 2002.

Cisco Systems Inc., “Quick Reference Guide: Cisco Aironet 340 Series Products.” [http://www.cisco.com/warp/public/cc/pd/witc/ao340ap/prodlit/aiqrg_rg.htm] January 2001

D'agostino, Debra, “Wireless (In)security: Is Your Network Snoop-Proof?” [http://www.cioinsight.com/article2/0,3959,394702,00.asp]. July 2002.

Denning, Dorothy E. and MacDoran, Peter F., “Location-Based Authentication: Grounding Cyberspace for Better Security.” [http://www.cs.georgetown.edu/~denning/infosec/Grounding.txt]. February 1996.

Flickenger, Rob, “Antenna on the Cheap (er, Chip).” [http://www.oreillynet.com/cs/weblog/view/wlg/448]. July 2001.

Fluhrer, Scott, et al, “Weaknesses in the Key Scheduling Algorithm of RC4” University of Maryland, 2001.

Geier, Jim, Wireless LAN Workshop Presentation Graphics, 2002.

Hopper, D. Ian, “Bush Adviser Urges Hackers to Locate Software Soft Spots,” [http://seattletimes.nwsource.com/html/businesstechnology/134504335_hack010.html]. August 2002

IEEE LAN MAN Standards Committee, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Computer Society, 1999.

Intel Corporation, “Wireless Security and VPN: Why VPN is Essential for Protecting Today’s 802.11 Networks,” Intel Corporation, 2002.

Interlink Networks, “A Practical Approach to Identifying and Tracking Unauthorized 802.11 Cards and Access Points,” Ann Arbor, MI, Intelink Networks Inc., 2002.

Intersil Corporation, Direct Sequence Spread Spectrum Baseband Processor with Rake Receiver and Equalizer (HFA3863) Data Sheet.” [http://www.intersil.com/data/fn/fn4/fn4856/fn4856.pdf]. December 2001.

Intersil Corporation, “PRISM 2 WLAN Chip Set Web Page.” [http://www.intersil.com/design/prism/ser-pii-11mbps.asp]. Accessed: August 2002.

Ipswitch Corporation, “WS_Ping Pro Pack Web Page.” [http://www.ipswitch.com/Products/WS_Ping/index.html]. Accessed: August 2002.

Maxim, Merritt and Pollino, David, Wireless Security. McGraw-Hill/Osborne, Berkeley, CA, 2002.

Pollino, David, Wireless Network Security, @STAKE Academy, Boston, MA, 2002.

Seattle Wireless Net, “Cisco Aironet.” [http://www.seattlewireless.net/index.cgi/CiscoAironet]. August 2002

Shipley, Peter, “Pete’s Demo Wardriving Maps.”[http://www.dis.org/wl/maps/]. Accessed: September 2002.

Shmoo Group, “Global Access Wireless Database.”[http://www.shmoo.com/cgi-bin/gawd/gawd.cgi/]. July 2001.

Symbol Technologies, “Wireless Products.” [http://www.symbol.com/products/wireless/wireless_sp24_11mbps.html]. 2002.

Yokoyama, Melvin K. Jr., Airborne Exploitation of an IEEE 802.11b Wireless Local Area Network. Master’s Thesis, Naval Postgraduate School, Monterey, California, September 2001.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

Bluetooth Special Interest Group, “The Official Bluetooth Website.” [http://www.bluetooth.com/dev/specifications.asp]. 2001.

Borisov, Nikita et al, “Security of the WEP Algorithm.” [http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html]. Accessed: August 2002.

Briney, Andy, “Securing Air.” [http://www.infosecuritymag.com/2002/jan/columns_note.shtml]. January 2002.

Geier, Jim, “802.11 WEP Concepts and Vulnerability.” [http://www.80211-planet.com/tutorials/article/0,4000,10724_1368661,00.html]. June 2002.

Geier, Jim, “Making Sense of Competing Wireless Standards: 802.11a or 802.11b.” [http://www.smallbusinesscomputing.com/buyersguide/article.php/1437401]. August 2002.

Harris, Blake M., “AMULET: Approximate Mobile User Location tracking System.” [http://www.csug.rochester.edu/~bharris/amulet/Amulet.pdf]. Accessed: August 2002

Kim, Byung-Seo and Ji Baowei, “Comparison FHSS vs. DSSS based on Simulation.” [http://my.netian.com/~jsnbs/class_project/eel6503.pdf]. December 2000.

Pearson, Bob, “Complementary Code Keying Made Simple.” [http://www.intersil.com/data/an/an9/an9850/AN9850.pdf]. November 2001.

Tessen, Robt. J.”Sam” et al., “Computer Dictionary, Technology and Telecommunications.” [http://www.orca.state.tx.us/PDF/OTS/Computer%20Dictionary.pdf] Accessed: September 2002.

The Cable Guy, “IEEE 802.1X Authentication for Wireless Connections.” [http://www.microsoft.com/technet/treeview/default.asp?url=

/technet/columns/cableguy/cg0402.asp?frame=true]. April 2002.

Utell, Michael, “Wireless PTP Bridges.” [http://www.networkcomputing.com/1204/1204buyers2.html]. February 2001.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Center for INFOSEC Study and Research
   Naval Postgraduate School
   Monterey, California

4. J.D. Fulp
   Naval Postgraduate School
   Monterey, California

5. Daniel C. Boger
   Naval Postgraduate School
   Monterey, California

6. Raymond R. Buettner
   Naval Postgraduate School
   Monterey, California

7. D. Curtis Schleher
   Naval Postgraduate School
   Monterey, California

8. Richard W. Adler
   Naval Postgraduate School
   Monterey, California

9. Commanding Officer
   Fleet Information Warfare Center
   Norfolk, Virginia

10. Officer in Charge
    Fleet Information Warfare Center Detachment
    Coronado, California

11. Darwin Engwer
    Nortel Networks
    Santa Clara, California

THIS PAGE INTENTIONALLY LEFT BLANK